(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 732 126**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.07.2014 PCT/EP2014/064971**

(87) Fecha y número de publicación internacional: **26.02.2015 WO15024706**

(96) Fecha de presentación y número de la solicitud europea: **11.07.2014 E 14747533 (9)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2019 EP 3036876**

(54) Título: **Aprovisionamiento asíncrono de claves de un dispositivo seguro a otro**

(30) Prioridad:

19.08.2013 US 201313969903

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.11.2019

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

CASTILLO, LAURENT;
LU, HONGQIAN KAREN y
ALI, ASAD MAHBOOB

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Aprovisionamiento asíncrono de claves de un dispositivo seguro a otro

Campo de la invención

La presente invención se refiere a un método para proporcionar de forma segura y asíncrona claves desde un dispositivo seguro de origen a un dispositivo seguro de destino a través de un servidor para el cual las claves que van a proporcionarse a través del método siguen siendo desconocidas para dicho servidor.

La invención también se refiere a un servidor de aprovisionamiento de claves útil para la implementación de dicho método.

Antecedentes de la invención

Junto con la proliferación de dispositivos móviles y servicios en la nube, el deseo de acceso en cualquier momento, en cualquier lugar y en cualquier dispositivo, y el rápido aumento de software maligno y ciberataques, la necesidad de aprovisionar claves criptográficas para los dispositivos se vuelve necesaria y crítica. Los servicios existentes aprovisionan claves desde un servidor de administración de claves a dispositivos. Esto deja aquellos servicios vulnerables que el servidor se vuelva comprometido. Sin embargo, actualmente no hay servicio que aprovisione claves de un dispositivo a otro tan pronto como los dos dispositivos no puedan comunicarse directamente entre sí.

En consecuencia, muchas situaciones no pueden ser abordadas actualmente por los sistemas conocidos. Entre estas situaciones, una persona que generalmente se autentica en la red de su compañía usando su computadora portátil con su tarjeta inteligente no puede hacer lo mismo desde su teléfono inteligente u otro dispositivo. La TI tendría que aprovisionar su teléfono inteligente usando sus credenciales corporativas en su tarjeta de identificación.

Las situaciones en las que las personas desean compartir archivos, entre personas o entre dispositivos, tampoco se abordan fácilmente. Por ejemplo, el archivo de una primera persona se almacena en un directorio compartido después del cifrado usando las claves almacenadas en la UICC en la tableta de la primera persona. La clave de cifrado para el archivo compartido debe transferirse de la UICC de la primera persona al elemento seguro (SE) de la segunda persona, para que esta segunda persona también pueda descifrar el archivo.

Las situaciones relacionadas con Internet de las cosas (IoT) también se encuentran, por ejemplo, cuando alguien que tiene un contador inteligente en casa quiere controlarlo desde su teléfono. Las configuraciones de los contadores inteligentes, las lecturas y los accionadores están protegidos mediante claves criptográficas. La empresa de servicios públicos que administra los contadores debe transferir estas claves al teléfono del propietario de la vivienda y debe poder actualizar las claves periódicamente.

También se preocupa por la invención el acceso a la nube seguro, ya que los proveedores de nube pública ofrecen API a sus clientes para controlar el acceso a sus recursos (almacenamiento, potencia informática, red). De hecho, estas API son la principal forma de acceder a los recursos de la nube. Las API están protegidas, cuando están aseguradas, con claves de API u otras claves criptográficas. La protección de estas claves es fundamental para la seguridad de los recursos de los clientes finales. El proveedor de la nube pública necesita una forma segura de transferir las claves de la API de su módulo de seguridad de hardware (HSM) de infraestructura a los dispositivos de los clientes finales.

Técnica anterior relevante

Se informa al lector interesado de que existen publicaciones de patentes, que describen técnicas anteriores a la invención, como por ejemplo US2004/062399-A1, US2013/156188-A1, WO2008/074366-A1, y US2008/049942-A1.

Compendio de la invención

La presente invención tiene como objetivo llenar la carencia actual de dicho servicio.

La presente invención se define, en su sentido más amplio, como un método que comprende los pasos de:

- activar una transferencia de clave en un servidor de aprovisionamiento de claves,

- para el servidor de aprovisionamiento de claves,

tomar una primera decisión de control de acceso para permitir o rechazar la transferencia de claves, y

si se permite la transferencia, enviar una notificación asíncrona de origen al dispositivo seguro de origen,

- cuando esté disponible, para el dispositivo seguro de origen,

cifrar una clave para ser transferida usando una clave de transporte para que solo el dispositivo seguro de destino pueda descifrar, y

enviar la clave cifrada al servidor de aprovisionamiento,

- para el servidor de aprovisionamiento,

tomar una segunda decisión de control de acceso, y

si se permite la transferencia, enviar una notificación asíncrona de destino al dispositivo seguro de destino,

- para el dispositivo seguro de destino, cuando esté disponible,

obtener la clave transferida cifrada, y

descifrar la clave transferida utilizando la clave de transporte.

Por lo tanto, el método según la presente invención propone utilizar un servidor de aprovisionamiento de claves que funcione de forma asíncrona con varios dispositivos y que no tenga conocimiento de las claves transferidas. El método de la invención permite que varios dispositivos confíen en un servidor central para gestionar la distribución de sus propias claves a una pluralidad de dispositivos o usuarios de forma segura. según la invención, la clave transferida y la clave de transporte solo son conocidas o conocidas por los dispositivos en cuestión. El servidor de aprovisionamiento y cualquier entidad en la ruta de comunicación nunca ven estas claves. Este esquema protege a los propietarios de claves, ya que las claves solo son accesibles por los dispositivos pretendidos. También es ventajoso para los desarrolladores y operadores del servidor de aprovisionamiento, ya que no necesitan preocuparse por las claves del cliente que solo están destinadas a los dispositivos de los clientes.

En una implementación ventajosa, dicho servidor es un servidor de aplicaciones web. Esta implementación concierne particularmente a cualquier aplicación de almacenamiento en la nube. La invención permite a cualquier dispositivo cifrar datos almacenados por servicios en la nube y compartir dichos datos con otros dispositivos. El uso de un servidor de aplicaciones web está especialmente adaptado a este contexto. Sin embargo, se puede observar aquí que cualquier modelo de servicio operado como se implementa en servidores debe ser adecuado para aplicaciones de almacenamiento en la nube.

Según una realización ventajosa, el método incluye además, después del envío de la notificación asíncrona de origen, los pasos de:

- para el dispositivo seguro de origen, cuando esté disponible, enviar una solicitud al servidor de aprovisionamiento para obtener información de la clave de transporte,

- para el servidor de aprovisionamiento, enviar información de la clave de transporte al dispositivo seguro de origen,

- para el dispositivo seguro de origen:

  - generar o recuperar la clave de transporte utilizando información de la clave de transporte,

  - cifrar la clave a transferir utilizando la clave de transporte,

  - enviar la clave cifrada y la información de transferencia de clave al servidor de aprovisionamiento.

La invención hace uso de la facultad para disociar la información de la clave de transporte, lo que permite a un dispositivo generar o recuperar la clave de transporte a partir de la propia información de la clave. Por lo tanto, el servidor de aprovisionamiento de claves almacena dicha información de clave de transporte y proporciona dicha información a uno o varios dispositivos cuando sea necesario.

Ventajosamente, el método incluye además, después del envío de la notificación asíncrona de destino, los pasos de:

- para el dispositivo seguro de destino, cuando esté disponible, enviar una solicitud al servidor de aprovisionamiento para obtener la clave transferida,

- para el servidor de aprovisionamiento, el envío de una información de transferencia de clave, que indica cómo la clave de transporte puede recuperarse o generarse por el dispositivo de destino, y la clave transferida cifrada al dispositivo seguro de destino,

- para el dispositivo seguro de destino, generar o recuperar la clave de transporte de la información de transferencia de clave y usar la clave de transporte para descifrar la clave transferida.

Estos pasos adicionales se adaptan al caso donde el dispositivo de origen también usó información de la clave de transporte para generar o recuperar la clave de transporte antes de cifrar la clave a transferir. Sin embargo, los pasos realizados en el lado de origen y los pasos realizados en el lado de destino pueden ocurrir independientemente uno del otro. La secuencia exacta de estos pasos dependerá del tipo de clave de transporte utilizada.

Según una realización preferida, la notificación asíncrona de origen comprende al menos un identificador de

notificación, una notificación de solicitud de transferencia de clave y un URI para que el dispositivo seguro de origen se conecte nuevamente.

Dicho contenido para la notificación asíncrona de origen es sencillo y proporciona al dispositivo de origen los elementos necesarios para implementar los pasos adicionales de la invención.

Según una realización preferida, la notificación asíncrona de destino incluye al menos una id de notificación, una información de evento de transferencia de clave y un URI para devolver una solicitud.

Este contenido para la notificación es sencillo y proporciona los elementos necesarios para continuar con los pasos de la invención.

En realizaciones específicas, las notificaciones asíncronas son a través de uno de los siguientes: Internet, web, SMS, notificaciones automáticas por teléfono, correo electrónico.

Esos medios de comunicación son comunes y pueden soportar la notificación de la invención.

Según una realización particular, la clave transferida cifrada es una clave de usuario asociada a un usuario y la información de la clave de transporte comprende un nombre de usuario.

Esta realización corresponde a la situación de un usuario que usa varios dispositivos para acceder a sus datos. El nombre de usuario permite a los dispositivos saber qué mecanismo de clave de transporte y qué clave de transporte se van a utilizar.

Según otra realización particular, la clave transferida es una clave secreta para compartirse por uno o más usuarios.

En este caso, el método de la invención se utiliza para transferir la clave secreta a cada uno de los dispositivos de la pluralidad de usuarios o para transferir la clave secreta a varios dispositivos de un mismo usuario para que compartan esta clave secreta y utilicen para un propósito previamente especificado.

En otra realización de la invención, la clave de transporte se recupera de un directorio como LDAP, Directorio Activo o cualquier otra base de datos.

Con esta realización, varias bases de datos conectadas están implicadas en la implementación de la invención y la invención permite confiar en la base de datos ya existente para desplegar un aprovisionamiento de claves como se define en la invención.

Según una característica particular, la clave transferida se cifra usando la clave pública del dispositivo seguro de destino.

Esta característica implica el despliegue de una criptografía asimétrica pero, entonces, permite muy sencillamente que el único dispositivo capaz de descifrar sea el correcto. Requiere que la clave que se transfiere se cifre con la clave correspondiente cada vez que se trate de un nuevo dispositivo de destino.

Según una realización específica, se genera una clave de contenedor de datos para cada contenedor de datos que se almacenará en un servicio en la nube.

Con esta realización, cada contenedor de datos tiene una clave correspondiente que permite intercambiar la clave de transporte utilizando esta clave de contenedor de datos. Una vez que se intercambia la clave de transporte, el intercambio de claves real puede tener lugar utilizando esta clave de transporte, de manera similar a otras realizaciones.

Al aplicar la invención, el dispositivo seguro se puede elegir del grupo formado por tarjetas inteligentes (que incluye varias formas de UICC), Módulo de Plataforma Confiable (TPM), Tarjeta Micro Secure Digital (Micro SD), Módulo de Seguridad de Hardware (HSM), Entorno de Ejecución Confiable (TEE), USB de testigo, elemento seguro incorporado (eSE).

La presente invención también se refiere a un servidor de aprovisionamiento de claves para implementar el método de una o varias de las reivindicaciones precedentes, incluyendo este servidor de aprovisionamiento al menos:

- un módulo de gestión del transporte,

- un módulo de control de acceso que toma una decisión de control de acceso para permitir o no la transferencia de claves,

- un módulo de notificación para enviar notificaciones asíncronas de origen y destino,

- una base de datos para almacenar al menos identificadores de usuario, metadatos de información de transporte, claves cifradas que se transferirán hasta el envío.

Un servidor de aprovisionamiento de claves de este tipo especializado a la gestión de claves puede procesar notificaciones asíncronas como se utiliza en la invención y almacenar los elementos necesarios para gestionar la información de claves de transporte, si es necesario.

Para la realización de los fines anteriores y relacionados, una o más realizaciones comprenden las características que se describen a continuación en detalle y se señalan particularmente en las reivindicaciones.

Breve descripción de los dibujos

La siguiente descripción y los dibujos adjuntos exponen en detalle ciertos aspectos ilustrativos y son indicativos de algunas de las diversas formas en que se pueden emplear los principios de las realizaciones. Otras ventajas y características novedosas se harán evidentes a partir de la siguiente descripción detallada cuando se consideren en conjunto con los dibujos y se pretende que las realizaciones descritas incluyan todos estos aspectos y sus equivalentes.

La figura 1 muestra esquemáticamente el contexto de la invención;

La figura 2 muestra un diagrama de flujo que describe el método de la invención;

La figura 3 muestra un diagrama de flujo que describe una realización específica de la invención; y

La figura 4 muestra esquemáticamente un servidor de aprovisionamiento de claves según la invención.

Descripción detallada de realizaciones de la invención

Los mismos elementos han sido designados con los mismos números de referencia en los diferentes dibujos. Para mayor claridad, solo los elementos y pasos que son útiles para la comprensión de la presente invención se han mostrado en los dibujos y se describirán. Además, cuando se dice que una acción se realiza por un dispositivo, de hecho se ejecuta por un microprocesador en este dispositivo controlado por códigos de instrucciones grabados en una memoria de programa en dicho dispositivo.

La figura 1 muestra esquemáticamente el contexto de la invención. La invención propone el aprovisionamiento seguro y asíncrono de claves desde un dispositivo de origen seguro SSD a otro dispositivo seguro, llamado dispositivo seguro de destino TSD. Para alcanzar este objetivo, la invención implementa un servidor de aprovisionamiento de claves KPS. El dispositivo seguro de origen y destino pueden ser de muchos tipos diferentes de dispositivos seguros, por ejemplo, tarjeta inteligente (UICC...), MicroSD segura, TEE, HSM, etc.

La figura 2 es un diagrama de flujo que representa el método de la invención. En un primer paso E1, se activa una solicitud de transferencia de clave en el servidor de aprovisionamiento de claves KPS. Esto se puede hacer de varias maneras. Por ejemplo, un usuario se conecta a la interfaz web de KPS del servidor o un servidor de aplicaciones llama a una API REST del servidor KPS. En otro ejemplo, el usuario interactúa con una aplicación móvil que se conecta al servidor KPS. El usuario desea que el servidor KPS transfiera una clave del dispositivo seguro de origen SSD a un dispositivo seguro de destino TSD. En la figura 2, la solicitud de transferencia se representa con una línea discontinua y se activa desde el dispositivo seguro de origen SSD.

En un segundo paso E2, se realiza un control de acceso AC1. Durante este paso, el servidor KPS toma la decisión de permitir o no la transferencia de claves. Este control de acceso AC1 incluye, pero no se limita a, la autenticación del usuario y/o el dispositivo y la aplicación de una política de control de acceso. La política de control de acceso puede incluir reglas, tal como, si el usuario tiene permiso para realizar la acción, si el dispositivo SSD tiene permiso para transferir una clave y si el propietario del dispositivo TSD tiene el privilegio o si el dispositivo TSD tiene el permiso para recibir la clave.

En el caso de que el control de acceso sea negativo (N), se informa al usuario del rechazo REF y se rechaza la solicitud. Si la decisión de control de acceso es positiva (Y), el servidor KPS continúa con el paso E3.

En este tercer paso E3, el servidor KPS envía una notificación asíncrona SAN al dispositivo SSD. Esta notificación asíncrona SAN incluye un id de notificación (por ejemplo, id1), una razón para la notificación (por ejemplo, "fuente de transferencia de clave") y el URI para que el dispositivo SSD se conecte nuevamente. Hay varias formas de enviar notificaciones, por ejemplo, a través de Internet, SMS, notificaciones automáticas por teléfono, correo electrónico, etc.

El dispositivo SSD puede estar ocupado cuando llega la notificación SAN o puede estar fuera de línea.

Una vez que procesa la notificación y está listo para responder, el dispositivo SSD pasa a la etapa E4. En este paso E4, encripta ENC el material de clave K que se transferirá utilizando una clave de transporte Kt.

Esta clave de transporte Kt se genera o recupera por el dispositivo SSD. Según la invención, esta clave Kt es tal que solo el dispositivo TSD puede descifrar los mensajes cifrados con ella.

En un paso E5, el dispositivo SSD envía el material de clave cifrado EK al servidor KPS. Ventajosamente, la

información de transferencia clave también se transfiere. Incluye, por ejemplo, el ID del dispositivo SSD, el ID del dispositivo TSD y la información de cifrado.

En la etapa E6, se realiza otro control de acceso AC2 y el servidor KPS toma la decisión de permitir o no la transferencia. Este control de acceso se puede implementar de una manera similar a la del paso E2.

De hecho, debido a que todo el flujo de trabajo es asíncrono, la situación puede haber cambiado desde que se inició el proceso. El control de acceso AC2 en esta etapa es importante. Si la decisión es positiva (Y), se realiza un paso E7. De lo contrario (N), el proceso se termina. En este último caso, puede ser ventajoso enviar una notificación de rechazo REF al dispositivo SSD si la transferencia activada se originó desde este dispositivo.

En la etapa E7, el servidor KPS envía una notificación TAN de forma asíncrona al dispositivo TSD informándole del evento de transferencia de clave. Incluye ventajosamente un nuevo id de notificación (id2) y un URI para devolver una solicitud.

El dispositivo TSD puede estar ocupado cuando llega la notificación TAN o puede estar fuera de línea. Una vez que procesa la notificación TAN y está listo para responder, en un paso E8, el dispositivo TSD envía una solicitud R(EK) para obtener la clave transferida al servidor KPS. El dispositivo TSD puede firmar digitalmente la solicitud R (EK).

En un paso E9, el servidor KPS envía la clave transferida cifrada. Puede firmar la respuesta.

El dispositivo TSD genera o recupera la clave de transporte Kt y la utiliza para descifrar DEC el material de clave transferido EK en el paso 10. El dispositivo TSD puede entonces almacenar y utilizar de forma segura el material criptográfico transferido K.

Ventajosamente, el servidor KPS elimina el material de clave cifrado transferido EK.

Las comunicaciones entre las entidades SSD, TSD, KPS deben protegerse usando protocolos de comunicación seguros, tal como SSL, TLS, HTTPS y otros protocolos de mensajería segura. Las entidades también pueden usar métodos fuera de banda, como OTP para ayudar a establecer comunicaciones seguras.

Según una realización ventajosa descrita en la figura 3, se implementan pasos intermedios. Estos pasos se relacionan con la gestión de claves de transporte.

Así, después de la recepción de la notificación asíncrona de origen en el paso E3, en un paso S1, el dispositivo SSD envía una solicitud R(Ktl) al servidor KPS para obtener la información de clave de transporte Ktl. El dispositivo SSD puede firmar digitalmente esta solicitud R (Ktl).

En respuesta, en un paso S2, el servidor KPS envía información de clave de transporte Ktl al dispositivo SSD. Esta información Ktl habilitará, en un paso S3, el dispositivo SSD para generar G(Kt) o recuperar R(Kt) la clave de transporte Kt que se usará para transferir K.

La información Ktl puede incluir, por ejemplo, el ID del dispositivo TSD, la propia clave pública de TSD o el ID del material criptográfico Kt requerido. El servidor KPS puede firmar digitalmente la respuesta.

Hay varias implementaciones en esta sección, siendo una lista no exhaustiva:

a. La clave de transporte es la clave pública del dispositivo TSD, estando esta clave pública e incluida directamente en Ktl

b. Un secreto compartido entre el dispositivo de origen SSD y el dispositivo de destino TSD, y Ktl contiene una ID de esta clave

c. Una clave derivada que solo pueden utilizar los dispositivos SSD y TSD, y Ktl contiene la ID secreta maestra y cualesquiera datos necesarios para la derivación.

d. El dispositivo SSD puede recuperar la clave de transporte de una base de datos segura o un directorio, basándose en la ID de TSD incluida en Ktl.

En esta realización, en la etapa E5 del método, el dispositivo SSD envía ventajosamente información de clave de transporte Ktl con el material de clave cifrado EK al servidor KPS.

En este caso, además de la solicitud R (EK), el dispositivo TSD realiza una solicitud R (Ktl) para la información de transferencia de clave KTI en un paso T1. Dicha información de transferencia clave KTI puede ser similar a la información clave de transporte Ktl, pero también puede diferir de esta información. Normalmente puede ser una selección de datos disponibles en la información de clave de transporte Ktl.

El servidor KPS responde así en un paso T2 enviando información de transferencia de clave KTI. En un paso T3, el dispositivo TSD genera G(Kt) o recupera R(Kt) la clave de transporte Kt basándose en la información de transferencia KTI. El mecanismo es ventajosamente similar al utilizado por el dispositivo SSD en el paso S3 en el caso de que la

información de la clave de transporte sea idéntica a la información de transferencia de clave Ktl.

Una vez que el dispositivo TSD también recibió el material de clave cifrado EK en el paso E9, podrá descifrar DEC el material de clave cifrado EK en un paso E10.

Cabe señalar que los pasos E8, E9, T1 y T2 se describieron por separado y en un orden específico. Sin embargo, estos pasos también pueden ser simultáneos. Por ejemplo, el mensaje enviado para transferir EK al dispositivo TSD también incluye información sobre el KTI de transferencia.

La figura 4 describe esquemáticamente un servidor KPS que implementa la invención. Este servidor KPS comprende un módulo de gestión de transferencia TMM que supervisa varios módulos destinados a implementar la invención. Esos módulos incluyen un módulo de control de acceso ACM para realizar los pasos E2 y E6 de la invención y un módulo de notificación NM destinado a procesar y enviar notificaciones asíncronas.

Este servidor también incluye una base de datos BD destinada a interactuar con el módulo de control de acceso ACM y el módulo de notificación NM. La base de datos BD almacena al menos identificadores de usuario, metadatos de información de transporte, claves cifradas que se transferirán hasta que se envíen. Finalmente, el servidor tiene ventajosamente un módulo criptográfico para firmar los mensajes que se envían desde KPS y para verificar los mensajes que se reciben por KPS, proporcionando una autenticación mutua entre los dispositivos SSD y TSD y el servidor KPS.

En la descripción detallada anterior, se hace referencia a los dibujos adjuntos que muestran, a modo de ilustración, realizaciones específicas en las que se puede poner en práctica la invención. Estas realizaciones se describen con suficiente detalle para permitir a los expertos en la técnica poner en práctica la invención. Debe entenderse que las diversas realizaciones de la invención, aunque diferentes, no son necesariamente excluyentes entre sí. La descripción detallada anterior, por lo tanto, no debe tomarse en un sentido limitativo, y el alcance de la presente invención se define solo por las reivindicaciones adjuntas, interpretadas de manera apropiada.

REIVINDICACIONES

1. Método para aprovisionar de forma segura y asíncrona las claves de un dispositivo seguro de origen a un dispositivo seguro de destino a través de un servidor de aprovisionamiento de claves (KPS) para el cual las claves que se aprovisionarán a través del método siguen siendo desconocidas, que comprende los pasos de:

- activar una transferencia de clave en el servidor de aprovisionamiento de claves (KPS),

- para el servidor de aprovisionamiento de claves (KPS), tomar una primera decisión de control de acceso para permitir o rechazar la transferencia de claves, incluyendo dicha primera decisión de control de acceso una primera autenticación de dicho dispositivo seguro de origen (SSD) o de un usuario de dicho dispositivo seguro de origen (SSD) y si se permite la transferencia, enviar una notificación de origen al dispositivo seguro de origen (SSD),

- para el dispositivo seguro de origen (SSD), recibir la notificación de origen, a continuación estar listo para responder y cuando esté listo para responder:

  cifrar una clave a transferirse usando una clave de transporte de modo que solo el dispositivo seguro de destino (TSD) pueda descifrar, y

  enviar la clave cifrada al servidor de aprovisionamiento de claves (KPS),

- para el servidor de aprovisionamiento de claves (KPS), tomar una segunda decisión de control de acceso, incluyendo dicha segunda decisión de control de acceso una segunda autenticación de dicho dispositivo seguro de destino (TSD) o de un usuario de dicho dispositivo seguro de destino (TSD) y si la transferencia está permitida, enviar una notificación de destino al dispositivo seguro de destino (TSD),

- para el dispositivo seguro de destino (TSD), recibir la notificación de destino, a continuación estar listo para responder y cuando esté listo para responder:

  obtener la clave transferida cifrada, y

  descifrar la clave transferida utilizando la clave de transporte.

2. Método según la reivindicación 1, en donde el servidor de aprovisionamiento de claves (KPS) es un servidor de aplicaciones web.

3. Método según una de las reivindicaciones 1 y 2, en donde el método incluye además, después del envío de la notificación de origen, los pasos de:

- para el dispositivo seguro de origen (SSD), cuando esté disponible, enviar una solicitud al servidor de aprovisionamiento de claves (KPS) para obtener información sobre la clave de transporte,

- para el servidor de aprovisionamiento de claves (KPS) enviar información de la clave de transporte al dispositivo seguro de origen (SSD),

- para el dispositivo seguro de origen (SSD), generar o recuperar la clave de transporte utilizando información de clave de transporte; cifrar la clave a transferir utilizando la clave de transporte; enviar la clave cifrada y la información de transferencia de clave al servidor de aprovisionamiento de claves (KPS).

4. Método según una de las reivindicaciones precedentes, en donde el método incluye además, después del envío de la notificación de destino, los pasos de:

- para el dispositivo seguro de destino (TSD), cuando esté disponible, enviar una solicitud al servidor de aprovisionamiento de claves (KPS) para obtener la clave transferida,

- para el servidor de aprovisionamiento de claves (KPS), enviar la información de transferencia de claves, que indica cómo puede recuperarse o generarse la clave de transporte por el dispositivo seguro de destino (TSD), y la clave transferida cifrada al dispositivo seguro de destino (TDS),

- para el dispositivo seguro de destino (TDS), generar o recuperar la clave de transporte de la información de transferencia de clave y usar la clave de transporte para descifrar la clave transferida.

5. Método según una de las reivindicaciones precedentes, en donde la notificación de origen comprende al menos una id de notificación, una notificación de solicitud de transferencia de clave y un URI para que el dispositivo de origen seguro (SSD) se conecte de nuevo.

6. Método según una de las reivindicaciones precedentes, en donde la notificación de destino incluye al menos una id de notificación, una información de evento de transferencia de clave y un URI para devolver una solicitud.

7. Método según una de las reivindicaciones precedentes, en donde las notificaciones son a través de uno de los

siguientes: Internet, web, SMS, notificaciones automáticas por teléfono, correo electrónico.

8. Método según una de las reivindicaciones precedentes, en donde la clave transferida cifrada es una clave de usuario asociada al usuario y la información de la clave de transporte comprende un nombre de usuario.

9. Método según una de las reivindicaciones precedentes, en donde la clave transferida es una clave secreta para compartirse por uno o más usuarios.

10. Método según una de las reivindicaciones precedentes, en donde la clave de transporte se recupera de un directorio como LDAP, Directorio Activo o cualquier otra base de datos.

11. Método según una de las reivindicaciones precedentes, en donde la clave transferida se cifra utilizando la clave pública del dispositivo seguro de destino (TDS).

12. Método según una de las reivindicaciones precedentes, en donde se genera una clave de contenedor de datos para cada contenedor de datos a almacenar en el servicio en la nube.

13. Método según una de las reivindicaciones anteriores, en donde los dispositivos seguros se eligen del grupo formado por tarjetas inteligentes, como por ejemplo UICC y otros, Módulo de Plataforma Confiable TPM, Tarjeta Micro Secure Digital MicroSD, Módulo de Seguridad de Hardware HSM, Entorno de Ejecución Confiable TEE, testigo USB, elemento seguro incorporado eSE.

14. Un servidor de aprovisionamiento de claves (KPS) para implementar el método de una o varias de las reivindicaciones anteriores, este servidor de aprovisionamiento de claves (KPS) incluye al menos:

- un módulo de gestión del transporte (TMM),

- un módulo de control de acceso (ACM) que toma una decisión de control de acceso para permitir o no la transferencia de claves,

- un módulo de notificación (NM) para enviar notificaciones de origen y destino,

- una base de datos (BD) para almacenar al menos identificadores de usuario, metadatos de información de transporte, claves cifradas que se transferirán hasta el envío.

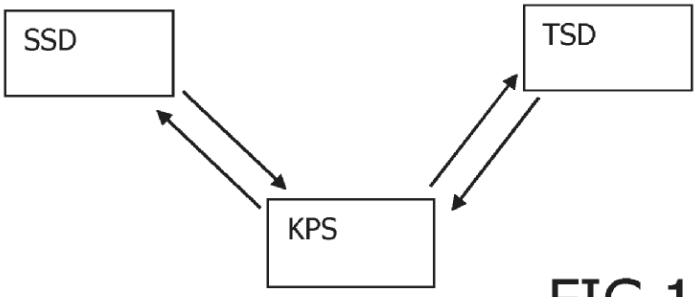

FIG.1

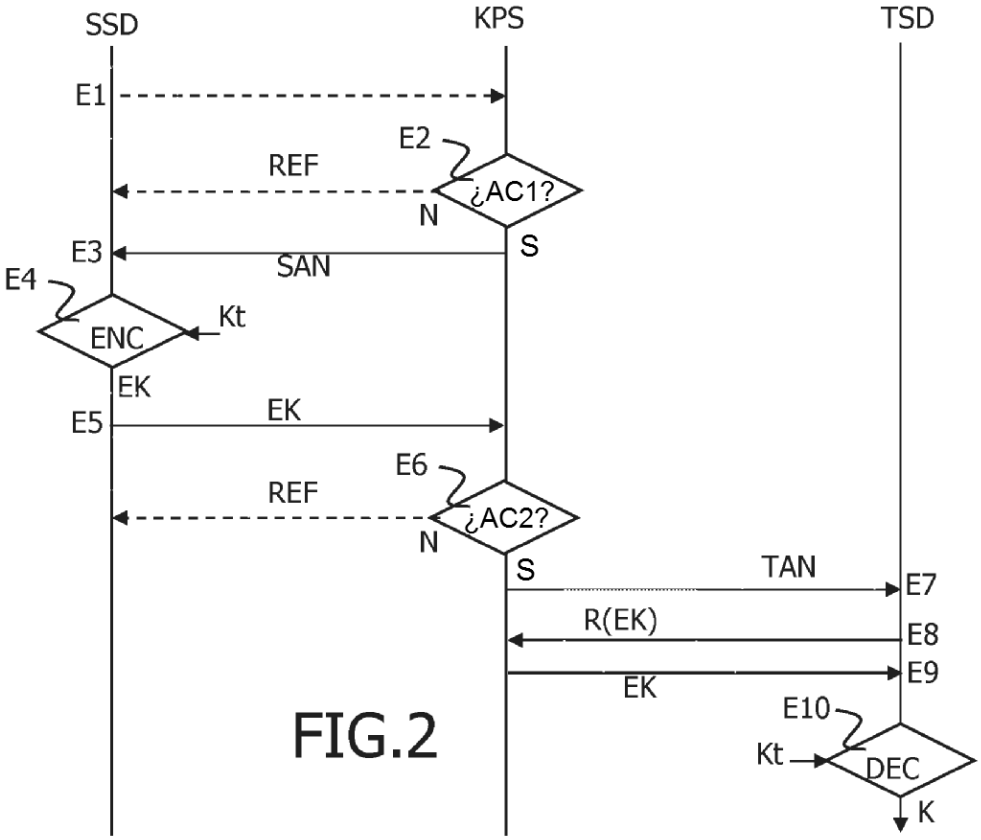

FIG.2

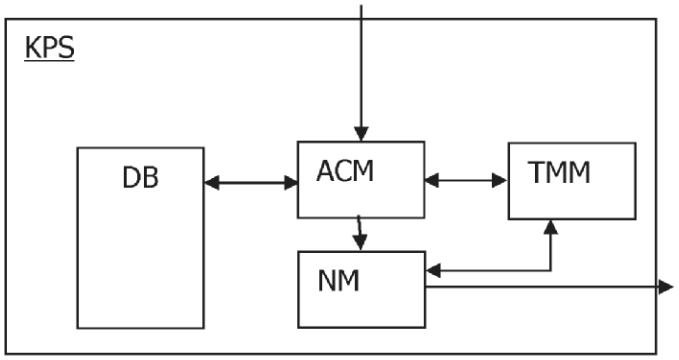

FIG.4

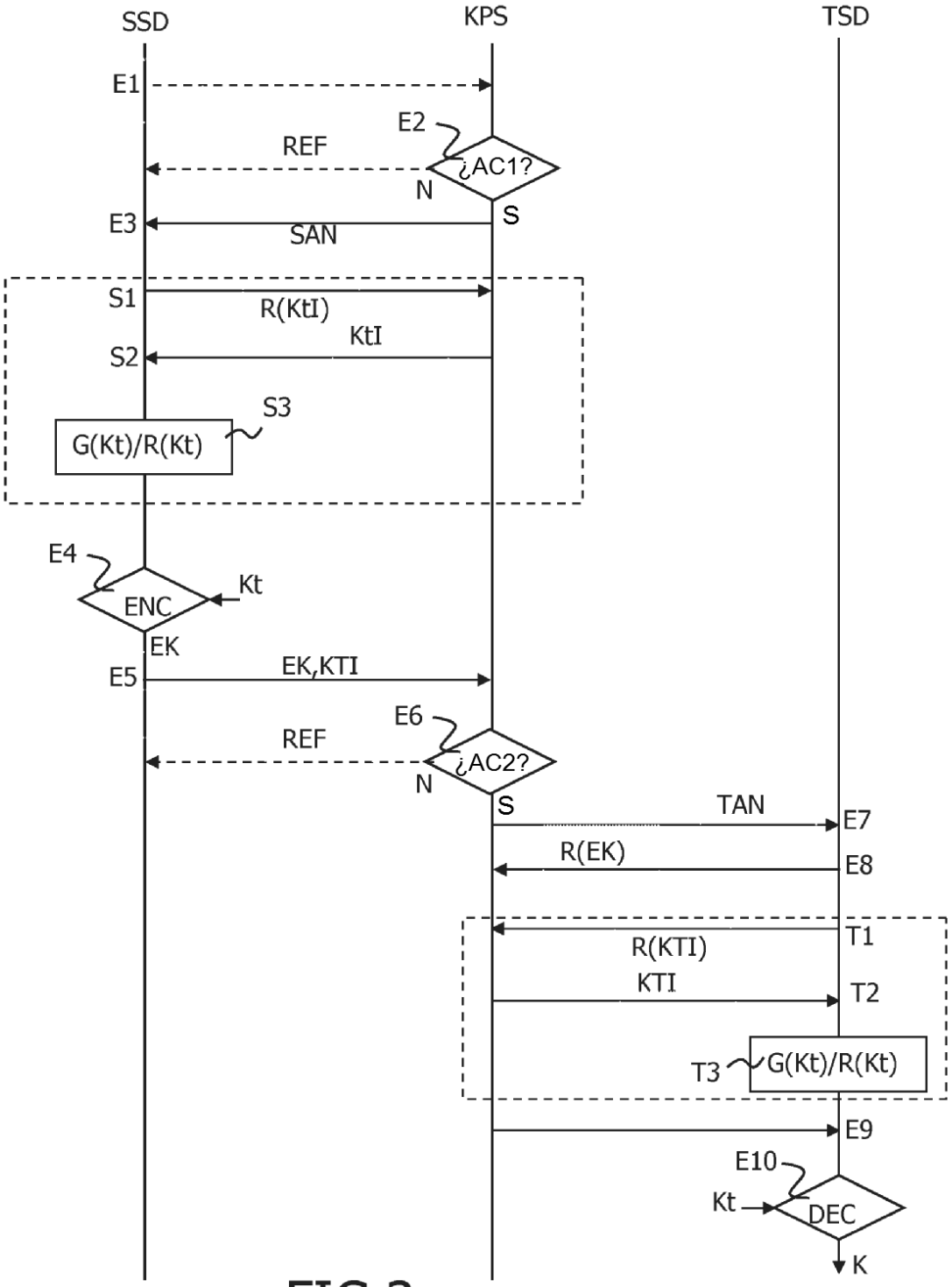
SSD
KPS
TSD
E1
E2
REF
¿AC1?
N
S
E3
SAN
S1
R(KtI)
KtI
S2
S3
G(Kt)/R(Kt)
E4
ENC
Kt
EK
E5
EK,KTI
E6
REF
¿AC2?
N
S
TAN
E7
R(EK)
E8
T1
R(KTI)
KTI
T2
T3
G(Kt)/R(Kt)
E9
E10
Kt
DEC
K

FIG.3