(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 727 014**

(51) Int. CI.:

H04N 7/167 (2011.01)
G06F 21/00 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.05.2008 E 08157182 (0)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 2129115**

(54) Título: **Método de actualización de datos de seguridad en un módulo de seguridad y módulo de seguridad para la ejecución de este método**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.10.2019

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

JUNOD, PASCAL y
BRIQUE, OLIVIER

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de actualización de datos de seguridad en un módulo de seguridad y módulo de seguridad para la ejecución de este método

Campo técnico

[0001] La presente invención se refiere a un método de actualización de datos de seguridad en un módulo de seguridad por un centro de gestión. También se refiere a un módulo de seguridad destinado a procesar tales datos de seguridad.

Técnica anterior

[0002] De manera ampliamente conocida, los algoritmos de criptografía utilizados actualmente para generar firmas electrónicas se pueden clasificar según dos tipos distintos. Uno de estos tipos comprende los algoritmos llamados simétricos y el otro tipo contiene los algoritmos asimétricos. Los algoritmos simétricos tienen las características siguientes: utilizan una misma clave para calcular una firma y para verificar su autenticidad. La clave se puede elegir de manera aleatoria, lo que significa que es muy sencillo encontrar un gran número de claves diferentes.

[0003] Los algoritmos asimétricos utilizan claves diferentes, pero asociadas por ciertas propiedades matemáticas, para las operaciones de firma y de verificación, respectivamente. Una de las limitaciones conocidas de los algoritmos asimétricos es la dificultad para generar claves. De hecho, al contrario que las claves utilizadas para una firma simétrica, las claves asimétricas deben responder a ciertos criterios precisos que no son fáciles de cumplir. Por lo tanto, es difícil producir un gran número de claves diferentes.

[0004] Por regla general, los algoritmos simétricos requieren además un tiempo de procesamiento significativamente más corto que los algoritmos asimétricos, pero ofrecen un menor nivel de seguridad. De hecho, si un tercero ha descubierto el algoritmo simétrico y la clave, dicho tercero puede utilizar estas informaciones para producir nuevos datos y autentificarlos.

[0005] La patente US 2004/0190721 describe un sistema de acceso condicional que comprende un módulo de seguridad y una unidad central.

Descripción de la invención

[0006] La presente invención se propone realizar un método que permita un tiempo de procesamiento de datos (firma y verificación) lo más corto posible con el uso de un algoritmo de cifrado simétrico, ofreciendo un nivel de seguridad elevado comparable al ofrecido por un algoritmo asimétrico de firma.

[0007] También se propone realizar un módulo de seguridad que permita la ejecución de este método.

[0008] El objetivo de la invención se logra mediante un método de actualización de datos de seguridad en un módulo de seguridad por un centro de gestión, método que comprende las etapas siguientes:

- definición de un algoritmo de cifrado simétrico C,
- definición de un algoritmo de descifrado simétrico D correspondiente a dicho algoritmo de cifrado C,
- definición de una clave K idéntica para el cifrado y el descifrado por medio de los algoritmos correspondientes definidos previamente,

caracterizado por el hecho de que se implementa en el módulo de seguridad, donde dicho algoritmo de descifrado D en forma de un módulo de descifrado material contiene únicamente los elementos lógicos relacionados con el descifrado.

[0009] El objetivo de la invención también se logra mediante un módulo de seguridad destinado a procesar datos de actualización transmitidos por un centro de gestión, caracterizado por el hecho de que incluye un módulo de descifrado material que contiene únicamente elementos lógicos relacionados con el descifrado de dichos datos de actualización y de que no contiene elementos lógicos relacionados con el cifrado de estos datos de actualización.

[0010] Según la presente invención, el módulo de seguridad contiene todos los elementos necesarios para la verificación de datos que se han firmado por medio de un algoritmo de cifrado simétrico, es decir, que contiene únicamente una de las dos direcciones de cifrado. De esta manera, los datos recibidos por este módulo de seguridad se pueden verificar rápidamente. Esta rapidez de autentificación es particularmente útil cuando se debe verificar un gran número de datos a la vez o cuando no se debe utilizar el módulo de verificación durante un largo período. Esto puede ser el caso en particular en el dominio de la televisión de acceso condicional.

[0011] En cambio, el módulo de seguridad no contiene los elementos necesarios para la firma de datos. Así, una persona malintencionada que haya podido acceder a los datos de verificación del módulo de seguridad no podrá acceder a las informaciones que permiten la operación de firma. De este modo, esta persona no podrá formar datos falsificados que confieran, por ejemplo, derechos de acceso de manera ilegal.

Breve descripción de los dibujos

[0012] La presente invención y sus ventajas se entenderán mejor en referencia a las figuras adjuntas y a la descripción detallada de una forma de realización particular, en las cuales:

- la figura 1 ilustra la preparación de datos de seguridad utilizados en el método de la invención; y
- la figura 2 representa el procesamiento de los datos recibidos por el módulo de seguridad de la invención.

Manera de realizar la invención

[0013] El módulo de seguridad de la invención se encarga del procesamiento de datos de actualización o de los datos de seguridad. Según esta invención, este módulo de seguridad incluye un módulo de descifrado material simétrico encargado de la verificación de los datos. Al contrario que los módulos similares del estado de la técnica, éste contiene únicamente los elementos lógicos necesarios para el descifrado de datos. De esta manera, este módulo no podrá realizar un cifrado.

[0014] Existe muchos algoritmos de cifrado simétricos utilizados o aplicados en módulos tales como tarjetas inteligentes, tarjetas con circuito integrado u otros módulos de seguridad. Entre estos algoritmos, se pueden citar en particular IDEA, DES, 3DES, AES u otros. Estos algoritmos utilizan de manera convencional registros de desplazamiento, módulos de sustitución y módulos de transposición en particular.

[0015] Estos elementos normalmente se utilizan para generar secuencias pseudoaleatorias a partir de un dato de inicialización (*seed*) o de una clave precedente. Estas secuencias pseudoaleatorias pueden luego ser utilizadas para formar claves utilizadas con un algoritmo de cifrado simétrico.

[0016] Según la invención, cuando se ha utilizado un valor de inicialización o una clave para generar una nueva clave, como se ha indicado antes, los datos de seguridad se pueden cifrar mediante esta clave generada.

[0017] Durante el descifrado, el orden de las operaciones utilizadas para generar una clave se invierte. En particular, si durante el cifrado se termina por un desplazamiento seguido de una sustitución, el descifrado comenzará por una sustitución seguida de un desplazamiento. Además, si el desplazamiento se hace hacia la izquierda durante el cifrado, se hará hacia la derecha en el descifrado.

[0018] Los detalles de los elementos que implementan los procedimientos de cifrado y de descifrado, es decir, el tipo de transposiciones, de sustituciones y de desplazamiento en particular, pueden estar definidos en una norma o en estándares correspondientes al algoritmo elegido, pero también pueden ser de tipo propietario. Una manera relativamente cómoda de realizar un módulo de descifrado propietario consiste en modificar ciertos parámetros tales como el número de registros de desplazamiento, el sentido o la cantidad del desplazamiento, el número de módulos de sustitución o de transposición, los parámetros ligados a la sustitución o a la transposición, a la vez que se mantiene un nivel de seguridad criptográfica equivalente.

[0019] Según la invención, solo es viable el descifrado en el módulo de descifrado del módulo de seguridad. Para que solo sea posible el descifrado, no se implementan en este módulo de descifrado los medios necesarios para efectuar las operaciones inversas al descifrado. Eso significa que, por ejemplo, si el descifrado utiliza un desplazamiento hacia la derecha en un registro de desplazamiento, no se implementarán en el módulo de descifrado los medios que permiten efectuar un desplazamiento hacia la izquierda. El mismo principio se aplica para los módulos de sustitución y de transposición en particular.

[0020] La invención también se refiere a un método para la actualización de los datos de seguridad en el módulo de seguridad descrito anteriormente. Este método incluye tres fases. La primera fase consiste en preparar los datos de actualización con el fin de enviarlos a uno o varios módulos de seguridad. La segunda fase consiste en enviar estos datos a los módulos de seguridad correspondientes. Esta fase es convencional y no se describe en detalle en la continuación del texto. La tercera fase consiste en procesar los datos recibidos por el módulo de seguridad, con el fin de realizar la actualización de este módulo.

[0021] La preparación de los datos se desarrolla de la manera siguiente. Los datos tienen al menos una parte útil PU. En primer lugar, se determina una huella EP a partir de esta parte útil. La determinación de la huella puede hacerse de varias maneras diferentes utilizando diferentes operaciones. En particular, es posible aplicar una función hash a toda o parte de la parte útil, retirar un determinado número de bits de esta parte útil, aplicar una función criptográfica o matemática a la parte útil, por ejemplo. Esta huella EP a continuación se cifra mediante una clave K con el fin de obtener una firma SG correspondiente a la parte útil PU inicial.

[0022] Los datos de seguridad según la invención a continuación se forman a partir de la parte útil PU y de la firma. También se puede agregar otros elementos, en particular un encabezado o datos de llenado, por ejemplo. Los datos de seguridad se pueden formar por la concatenación de diferentes elementos mencionados anteriormente o por otras operaciones conocidas.

[0023] Cuando los datos de seguridad se han formado, se pueden enviar al módulo de seguridad correspondiente o a varios módulos según la aplicación. Estos datos habitualmente se cifran con una clave que puede ser propia del sistema o en particular con una clave de sesión.

[0024] Cuando un módulo de seguridad correspondiente ha recibido los datos de seguridad preparados y enviados según las etapas anteriores, éste verifica en primer lugar su autenticidad. Para ello, la firma SG' de los datos recibidos se extrae. Ésta se descifra mediante la clave de cifrado K. El descifrado de esta firma proporciona una huella EP*. Se debe señalar que, debido al uso de un algoritmo de cifrado simétrico, la clave de cifrado K utilizada durante la preparación de los datos con el fin de su envío es la misma que la clave de descifrado K para utilizar en el módulo de seguridad.

[0025] Paralelamente, la parte útil PU' de los datos recibidos por el módulo de seguridad son procesados de manera idéntica en su procesamiento durante su preparación. Eso significa que, si se ha utilizado una función hash con clave para obtener la huella EP a partir de la parte útil PU en el centro de gestión, se utilizará la misma función hash con clave, con la misma clave en el módulo de seguridad. De este modo, se obtiene una huella EP'. La huella EP' así obtenida se compara con la huella EP* obtenida por descifrado de la firma. Si estas dos huellas se corresponden, el mensaje se acepta y los datos de actualización se implementan en el módulo de seguridad. Por el contrario, si las dos huellas no se corresponden, podría significar que el mensaje recibido no es un mensaje auténtico. Por lo tanto, es rechazado. Cuando el mensaje ha sido aceptado, los datos que contiene se pueden utilizar de manera convencional.

REIVINDICACIONES

1. Método de actualización de datos de seguridad en un módulo de seguridad por un centro de gestión, en el cual los datos de seguridad comprenden al menos una parte útil PU, método que comprende las etapas siguientes:

- definición de un algoritmo de cifrado simétrico C,
- definición de un algoritmo de descifrado simétrico D correspondiente a dicho algoritmo de cifrado C,
- definición de una clave K idéntica para el cifrado y el descifrado por medio de los algoritmos correspondientes definidos previamente,

caracterizado por el hecho de que se implementa en el módulo de seguridad dicho algoritmo de descifrado D en forma de un módulo de descifrado material que contiene únicamente los elementos lógicos relacionados con el descifrado, donde este método también está **caracterizado por el hecho de que** incluye las etapas siguientes:

- recepción, por el módulo de seguridad, de los datos de seguridad formados por la parte útil y una firma SG correspondiente a la parte útil;
- extracción de la firma de dichos datos de seguridad;
- descifrado de la firma extraída por dicho algoritmo de descifrado simétrico D,
- extracción de la parte útil de los datos de seguridad recibidos;
- determinación de una huella a partir de la parte útil, huella que se determina de manera idéntica a la determinación de una huella en una fase de preparación de los datos;
- comparación de la huella y de la firma descifrada;
- aceptación o rechazo de los datos según el resultado de la comparación.

2. Método según la reivindicación 1, método **caracterizado por el hecho de que** incluye la fase de preparación de los datos de seguridad para su envío por el centro de gestión y una fase de envío de dichos datos de seguridad, donde la fase de preparación de los datos de seguridad comprende las etapas siguientes:

- determinación de una huella EP a partir de dicha parte útil PU;
- cifrado de la huella EP con el fin de obtener una firma SG por dicho algoritmo de cifrado simétrico C;
- formación de dichos datos de seguridad SDT a partir de la parte útil PU y de la firma SG;
- envío al módulo de seguridad de dichos datos de seguridad SDT.

3. Método según la reivindicación 2, **caracterizado por el hecho de que** la huella se determina a partir de la parte útil por medio de una función hash.

4. Método según la reivindicación 3, **caracterizado por el hecho de que** la función hash es una función hash con clave.

5. Método según la reivindicación 1, **caracterizado por el hecho de que** los datos de seguridad se envían en forma cifrada al módulo de seguridad.

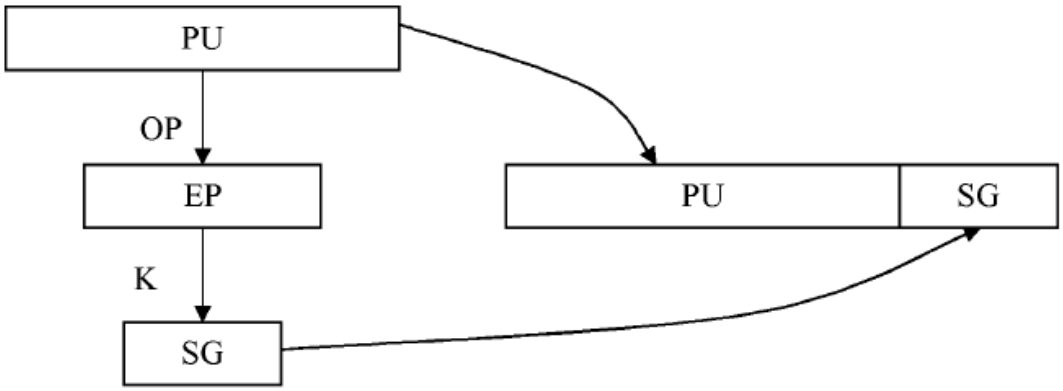

FIG. 1

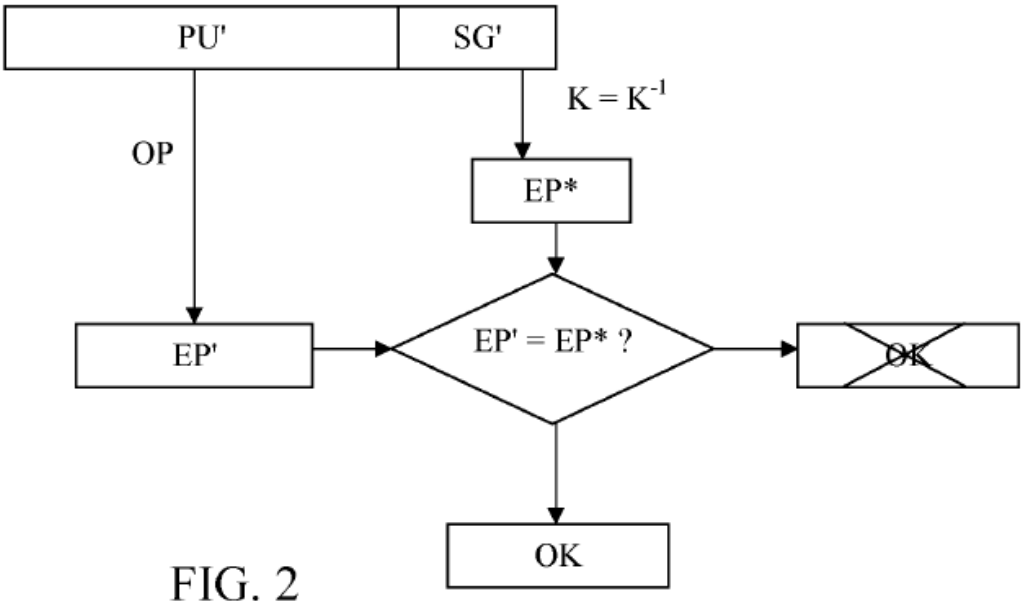

FIG. 2