(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 396**

(51) Int. CI.:

G06F 21/57 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.02.2016 E 16155540 (4)**

(97) Fecha y número de publicación de la concesión europea: **13.06.2018 EP 3206154**

(54) Título: **Métodos y dispositivos para la transferencia segura de datos útiles**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2018

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

FUCHS, BURKHARD;
STÜCKER, OLAF;
KÜGLER, DENNIS y
KLEIN, DOMINIK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Métodos y dispositivos para la transferencia segura de datos útiles

La invención se refiere a métodos y dispositivos para la transferencia segura de datos útiles. En particular la invención se refiere a un método para la transferencia segura de datos útiles desde un sistema en segundo plano, en particular un servidor, a un elemento de seguridad, un sistema en segundo plano, en particular un servidor, para la transferencia segura de datos útiles a un elemento de seguridad así como a un elemento de seguridad correspondiente.

Los elementos de seguridad en forma de tarjetas con chip se emplean con frecuencia como documentos de seguridad, por ejemplo en forma de un documento de identidad electrónico, de una tarjeta con firma o similar. En este sentido los elementos de seguridad modernos disponen por regla general de una memoria así como de un procesador y están configurados mediante un sistema operativo para ejecutar aplicaciones de seguridad. Ejemplos de aplicación para tales aplicaciones de seguridad son una autenticación con respecto a un terminal, el establecimiento de un canal de comunicación de datos asegurado, la firma electrónica de datos así como la verificación de firmas y similares. De este modo tales elementos de seguridad pueden utilizarse para interactuar con proveedores de servicios discrecionales, para autenticarse por ejemplo para transacciones electrónicas, por ejemplo a través de Internet y ejecutarlas de manera segura. Adicionalmente pueden utilizarse elementos de seguridad para el almacenamiento de datos, como por ejemplo datos personales y/o relevantes para la seguridad así como otros datos útiles y respaldar por ejemplo sistemas de control de fronteras o de control de acceso.

Con frecuencia los elementos de seguridad disponen de una interfaz de comunicación adecuada, por ejemplo una interfaz de comunicación RF-o NFC para poder comunicarse sin contacto con un terminal o un servidor de un sistema en segundo plano conectado con el terminal.

En sistemas operativos para PC se sabe cómo reequipar o modificar mediante actualizaciones de software por un lado la funcionalidad de un sistema operativo y por otro lado mejorar mecanismos de seguridad, por ejemplo mediante el cierre de fallos de seguridad descubiertos. A este respecto un mecanismo de actualización de software comprende habitualmente una prueba de autenticidad, con lo que puede garantizarse que solo se instalen tales actualizaciones de software cuya autenticidad está garantizada por el fabricante de la actualización.

En el marco de elementos de seguridad, en particular tarjetas con chip, se conocen actualizaciones de software, que actualizan o amplían la funcionalidad de los elementos de seguridad, es decir de las aplicaciones implementadas en el elemento de seguridad, que se ejecutan en el sistema operativo del elemento de seguridad. Un mecanismo de actualización de software puede comprenden en este campo igualmente una prueba de autenticidad. Se conocen estándares correspondientes para una gestión de aplicación de este tipo en elementos de seguridad, por ejemplo el estándar "*Global Platform Specification*". Según este estándar se instala la actualización de software, al establecerse entre un servidor de un sistema en segundo plano y el elemento de seguridad una conexión encriptada. Los datos de actualización sin encriptar existentes en el servidor se transmiten entonces a través de la conexión con el elemento de seguridad y se instalan tras una prueba de autenticidad realizada con éxito.

En varios escenarios de aplicación se emiten elementos de seguridad durante un largo periodo de tiempo. Por ejemplo pueden operarse elementos de seguridad en forma de documentos de identidad electrónicos durante un periodo de tiempo de diez años o más en el campo. No ha de descartarse que durante tales largos periodos de tiempo los mecanismos de seguridad originales del sistema operativo de un elemento de seguridad pierdan su eficacia o incluso se vean comprometidos por completo, entre otros mediante fallos de seguridad descubiertos en el hardware o en el sistema operativo del elemento de seguridad. Además también los avances técnicos y/o criptoanalíticos pueden llevar a que la seguridad de los métodos criptográficos empleados en el momento de emisión de un elemento de seguridad se vea perjudicada, por ejemplo debido a longitudes de clave demasiado cortas y/o avances técnicos y/o criptoanalíticos que hacen posible debido a fenómenos que pueden observarse físicamente comprometer la funcionalidad de seguridad de un elemento de seguridad mediante un denominado ataque de canal lateral.

A menudo los problemas de seguridad de este tipo pueden eliminarse mediante actualizaciones de software de los mecanismos de seguridad del sistema operativo de un elemento de seguridad. La utilización directa de técnicas establecidas de actualizaciones de software para sistema operativos de PC o para aplicaciones sobre elementos de seguridad lleva no obstante en este sentido a los siguientes problemas.

Un mecanismo de actualización de software puede servir incluso a un atacante como canal lateral o simplificar un ataque mediante análisis de canal lateral, cuando el mecanismo permite a un atacante realizar operaciones criptográficas con la funcionalidad de seguridad del elemento de seguridad utilizada en el momento de la actualización de software y posiblemente debilitada para generar fenómenos que puedan observarse físicamente. Además un mecanismo de actualización de software debe garantizar que el carácter confidencial de los datos de actualización esté presente continuamente desde el momento de la creación en el lado del fabricante hasta la activación tras la transferencia al elemento de seguridad. Si un atacante obtiene acceso a los datos de actualización,

entonces mediante ingeniería inversa pueden extraerse conclusiones directas sobre los fallos de seguridad del elemento de seguridad tomados como base. Un elemento de seguridad presenta por regla general tanto una capacidad de almacenamiento o comunicación limitada como una capacidad de cómputo restringida, lo que limita la complejidad de las operaciones criptográficas que pueden utilizarse en un mecanismo de actualización de software para elementos de seguridad. Finalmente un mecanismo de actualización de software debe garantizar que la autenticidad de los datos de actualización quede garantizada antes de la instalación en el elemento de seguridad.

Ante este trasfondo el objetivo de la presente invención es facilitar métodos y dispositivos mejorados para la transmisión segura de datos útiles, en particular de datos útiles en forma de una actualización de software para un elemento de seguridad.

Este objetivo se resuelve mediante las características de las reivindicaciones independientes. Las formas de perfeccionamientos ventajosos son objeto de las reivindicaciones dependientes.

Según un primer aspecto a la invención se refiere un método para la transferencia segura de datos útiles a un elemento de seguridad, comprendiendo el método: la facilitación de una clave de encriptación K_{ENC} y de una clave de valor de comprobación K_{MAC} en el elemento de seguridad; la encriptación de los datos útiles mediante la clave de encriptación K_{ENC} empleando un cifrado, para generar al menos un primer texto cifrado c_1 y un segundo texto cifrado c_2; la transferencia de un conjunto de datos al elemento de seguridad, comprendiendo el conjunto de datos transferido completamente el primer texto cifrado c_1, el segundo texto cifrado c_2, un valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación del segundo texto cifrado $h(c_2)$, un valor de comprobación de un primer valor de comprobación basado en claves $h(MAC_1)$, estando incluido en el primer valor de comprobación basado en claves MAC_1 el valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación de un segundo valor de comprobación basado en claves $h(MAC_2)$, estando incluido en el segundo valor de comprobación basado en claves MAC_2 el primer valor de comprobación basado en claves MAC_1 y el valor de comprobación del segundo texto cifrado $h(c_2)$, así como una firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves $Sign_1[h(c_1)||h(MAC_1)]$.

Según una forma de realización del primer aspecto de la invención en el primer valor de comprobación basado en claves MAC_1 está incluido además un parámetro de inicialización IV_{MAC}.

Según una forma de realización del primer aspecto de la invención en la etapa de la transferencia del conjunto de datos al elemento de seguridad se transfieren un primer mensaje, que comprende el valor de comprobación del primer texto cifrado $h(c_1)$ y el valor de comprobación del primer valor de comprobación basado en claves $h(MAC_1)$, y un segundo mensaje, que comprende el valor de comprobación del segundo texto cifrado $h(c_2)$ y el valor de comprobación del segundo valor de comprobación basado en claves $h(MAC_2)$, al elemento de seguridad.

Según una forma de realización del primer aspecto de la invención el primer mensaje comprende además la firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves $Sign_1[h(c_1)||h(MAC_1)]$.

Según una forma de realización del primer aspecto de la invención el método comprende las etapas adicionales, comprobar como respuesta a la transferencia del primer mensaje al elemento de seguridad la firma sobre del valor de comprobación del primer texto cifrado $h(c_1)$ y el valor de comprobación del primer valor de comprobación basado en claves $h(MAC_1)$ del elemento de seguridad y, en caso de que la firma del elemento de seguridad no pueda verificarse, el elemento de seguridad interrumpe el proceso.

Según una forma de realización del primer aspecto de la invención el segundo mensaje comprende el primer texto cifrado c_1.

Según una forma de realización del primer aspecto de la invención el conjunto de datos comprende además una firma sobre del valor de comprobación del segundo valor de comprobación basado en claves $Sign_2[h(MAC_2)]$.

Según una forma de realización del primer aspecto de la invención en la etapa de la transferencia del conjunto de datos al elemento de seguridad se transfiere un mensaje adicional al elemento de seguridad, que comprende la firma sobre del valor de comprobación del segundo valor de comprobación basado en claves $Sign_2[h(MAC_2)]$.

Según una forma de realización del primer aspecto de la invención en caso del valor de comprobación del primer texto cifrado se trata de un valor de resumen criptográfico (*hash*) del primer texto cifrado $h(c_1)$ y en caso del valor de comprobación del segundo texto cifrado se trata de un valor *hash* del segundo texto cifrado $h(c_2)$.

Según una forma de realización del primer aspecto de la invención en el caso del cifrado, que se emplea para la encriptación de los datos útiles mediante la clave de encriptación K_{ENC}, se trata de un cifrado por bloques y/o de un cifrado en flujo.

Según una forma de realización del primer aspecto de la invención en el caso del cifrado, que se emplea para la

encriptación de los datos útiles mediante la clave de encriptación K_{ENC}, se trata de un cifrado en flujo, que en una parte basada en claves del método genera un flujo de claves, mediante el cual en una parte del método no basada en claves se generan el primer texto cifrado c_1 y el segundo texto cifrado c_2.

Según una forma de realización del primer aspecto de la invención en el caso del cifrado, que se emplea para la encriptación de los datos útiles mediante la clave de encriptación K_{ENC}, se trata de un cifrado por bloques AES, en particular un cifrado por bloques AES en el modo OFB o modo CTR, o de un cifrado por bloques TDES.

Según una forma de realización del primer aspecto de la invención el primer valor de comprobación basado en claves y el segundo valor de comprobación basado en claves son un MAC, en particular un CMAC o CBC-MAC, y se calculan empleando el cifrado por bloques AES o el cifrado por bloques TDES que se emplea también para la encriptación.

Según una forma de realización del primer aspecto de la invención para la encriptación de los datos útiles mediante la clave de encriptación K_{ENC} y para la creación de los valores de comprobación basados en claves también puede emplearse un cifrado por bloques AES en el modo Galois/CTR.

Según una forma de realización del primer aspecto de la invención la facilitación de la clave de encriptación K_{ENC} y de la clave de valor de comprobación K_{MAC} en el elemento de seguridad comprende la etapa del cálculo de un secreto y la etapa de la derivación de la clave de encriptación K_{ENC} y de la clave de valor de comprobación K_{MAC} a partir del secreto calculado.

Según una forma de realización del primer aspecto de la invención el conjunto de datos comprende además una clave pública de un par de claves efímeras PA y comprendiendo la etapa del cálculo de un secreto comprende el cálculo del secreto basándose de la clave pública del par de claves efímeras PA y de una clave privada dB depositado de manera segura en el elemento de seguridad.

Según una forma de realización del primer aspecto de la invención el conjunto de datos comprende además una firma sobre de la clave pública del par de claves efímeras PA o al menos sobre de una parte significativa del mismo.

Según un segundo aspecto la invención se refiere a un elemento de seguridad con: una interfaz de comunicación, que está configurada para recibir un conjunto de datos transferido por un sistema en segundo plano, comprendiendo el conjunto de datos transferido completamente un primer texto de cifrado c_1, un segundo texto cifrado c_2, un valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación del segundo texto cifrado $h(c_2)$, un valor de comprobación de un primer valor de comprobación basado en claves $h(MAC_1)$, estando incluido en el primer valor de comprobación basado en claves MAC_1 el valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación de un segundo valor de comprobación basado en claves $h(MAC_2)$, estando incluidos en el segundo valor de comprobación basado en claves MAC_2 el primer valor de comprobación basado en claves MAC_1 y el valor de comprobación del segundo texto cifrado $h(c_2)$, así como una firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves $Sign_1[h(c_1)||h(MAC_1)]$; y un procesador, que está configurado para verificar basándose en una clave de encriptación K_{ENC} y en una clave de valor de comprobación K_{MAC} el conjunto de datos y desencriptar el primer texto cifrado c_1 y el segundo texto cifrado c_2.

Según un tercer aspecto la invención se refiere a un sistema en segundo plano, en particular un servidor, con: un procesador, que está configurado para encriptar datos útiles mediante una clave de encriptación K_{ENC} empleando un cifrado, para obtener al menos un primer texto cifrado c_1 y un segundo texto cifrado c_2; y una interfaz de comunicación, que está configurada para transferir un conjunto de datos a un elemento de seguridad, comprendiendo el conjunto de datos transferido completamente el primer texto cifrado c_1, el segundo texto cifrado c_2, un valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación del segundo texto cifrado $h(c_2)$, un valor de comprobación de un primer valor de comprobación basado en claves $h(MAC_1)$, estando incluido en el primer valor de comprobación basado en claves MAC_1 el valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación de un segundo valor de comprobación basado en claves $h(MAC_2)$, estando incluidos en el segundo valor de comprobación basado en claves MAC_2 el primer valor de comprobación basado en claves MAC_1 y el valor de comprobación del segundo texto cifrado $h(c_2)$, así como una firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves $Sign_1[h(c_1)||h(MAC_1)]$.

Otros ejemplos de realización se explican con referencia a los dibujos adjuntos. Muestran:

La figura 1, una representación esquemática de un sistema de comunicación con un servidor de un sistema en segundo plano y un elemento de seguridad según una forma de realización;
la figura 2, una representación esquemática de un método para la transmisión segura de datos útiles desde un servidor de un sistema en segundo plano a un elemento de seguridad según una forma de realización;
la figura 3, una representación esquemática de un conjunto de datos que puede emplearse para la transmisión segura de datos útiles desde un servidor de un sistema en segundo plano a un elemento de seguridad según una forma de realización; y

la figura 4, una representación esquemática del desarrollo de un posible método para la encriptación de los datos útiles en un sistema en segundo plano según una forma de realización.

En la siguiente descripción detallada se hace referencia a los dibujos adjuntos que forman una parte de esta y en los que se muestran como ilustración formas de realización específicas en las que puede realizarse la invención. Se entiende que también pueden utilizarse otras formas de realización y pueden llevarse a cabo variaciones estructurales o lógicas sin desviarse del concepto de la presente invención. La siguiente descripción detallada por lo tanto no ha de entenderse en un sentido limitativo. Además se entiende que las características de los diferentes ejemplos de realización descritos en la presente memoria pueden combinarse entre sí, siempre y cuando no esté indicado específicamente lo contrario.

Los aspectos y formas de realización se describen con referencia a los dibujos, refiriéndose los mismos números de referencia en general a los mismos elementos. En la siguiente descripción para fines descriptivos se representan numerosos detalles específicos para otorgar una comprensión extensa de uno o varios aspectos de la invención. Sin embargo para un experto en la materia puede ser obvio sin embargo que pueden realizarse uno o varios aspectos o formas de realización con un menor grado de detalles específicos. En otros casos se representan estructuras y elementos conocidos en forma esquemática para facilitar la descripción de uno o varios aspectos o formas de realización. Se entienden que pueden utilizarse otras formas de realización y llevarse a cabo variaciones estructurales o lógicas sin desviarse del concepto de la presente invención.

Se describen dispositivos, y se describen métodos. Se entiende que las propiedades básicas de los dispositivos también son válidas para los métodos y a la inversa. Por lo tanto para mayor brevedad se renuncia dado el caso a una descripción duplicada de tales propiedades.

La figura 1 muestra una representación esquemática de una forma de realización preferida de un elemento de seguridad 101 en forma de una tarjeta con chip en comunicación con un sistema en segundo plano, en particular un servidor 111, que configuran parte de un sistema de comunicación 100. Además del servidor 111 el sistema en segundo plano puede presentar componentes adicionales, en particular servidor y/o terminales en las cuales adicionalmente al servidor 111 pueden facilitarse algunas de las funcionalidades descritas a continuación. Preferiblemente se trata en el caso del elemento de seguridad 101 de un documento de seguridad electrónico, como por ejemplo un carné de identidad electrónico, un pasaporte electrónico, una tarjeta con firma o similar. Sin embargo en el caso del elemento de seguridad 101 puede es tratarse igualmente de una tarjeta con chip para realizar transacciones sin dinero en metálico, por ejemplo una tarjeta de débito o una tarjeta de crédito, o también una tarjeta SIM o un módulo SIM que están conectados puede insertarse o fijamente conectado por cables con un terminal móvil y sirven para la identificación del abonado de telefonía móvil.

La tarjeta con chip 101 representada en la figura 1 está configurada para intercambiar datos con el servidor 111. Por intercambio de datos se entiende en este caso una transmisión de señales, un control alterno y en casos sencillos también una conexión entre el servidor 111 y la tarjeta con chip 101. En la teoría de la información un intercambio de datos está marcado en particular mediante el modelo emisor-receptor: datos o informaciones se codifican en signos y se transmiten después por un emisor a través de un canal de transmisión a un receptor. En este sentido es decisivo que emisor y receptor empleen la misma codificación para que el receptor pueda decodificar los datos.

Para la comunicación entre la tarjeta con chip 101 y el servidor 111 del sistema en segundo plano tanto la tarjeta con chip 101 como el servidor 111 presentan interfaces de comunicación 105 y 113 adecuadas. Las interfaces 105 y 113 pueden estar diseñadas por ejemplo de modo que la comunicación entre estas o entre la tarjeta con chip 101 y el servidor 111 se realice al menos parcialmente sin contacto, es decir a través de la interfaz aérea, por ejemplo a través de una interfaz RF o NFC. En este caso la interfaz 105 de la tarjeta con chip 101 puede presentar una estructura de antena configurada de manera adecuada y la interfaz 113 del servidor o del sistema en segundo plano 111 puede comprender un aparato de lectura. En formas de realización adicionales la tarjeta con chip 101 puede conectarse a través de la interfaz 105 de modo galvánico, es decir por contacto, con la interfaz 113 del servidor o del sistema en segundo plano 111. En este caso la interfaz 105 comprende por regla general un campo de contacto dispuesto en un lado de la tarjeta con chip 101 con superficies de contacto para el intercambio de datos con el servidor 111 y la interfaz 113 del servidor o del sistema en segundo plano 111 un lector de tarjeta. Naturalmente por la presente invención también están comprendidos elementos de seguridad en forma de tarjetas con chip que presentan tanto una interfaz para la comunicación con contacto como una interfaz para la comunicación sin contacto y que se conocen como tarjetas con chip con interfaz dual.

En la forma de realización representada en la figura 1 la tarjeta con chip 101 comprende además de la interfaz 105 para la comunicación con el servidor o el sistema en segundo plano 111 un procesador 103, que está conectado en comunicación con la interfaz 105. Tal como se sabe entre las tareas primarias del procesador 103 se encuentran la ejecución de funciones aritméticas y lógicas y la lectura y escritura de datos, tal como se define mediante una aplicación de software que se ejecuta en el procesador 103. El procesador 103 puede estar conectado además con una memoria de trabajo volátil (RAM) 109 y una memoria 107 no volátil regrabable (denominada en la figura 1 "NVM" (*nonvolatile memory*)). En formas de realización de la invención en el caso de la memoria no volátil 107 puede tratarse de una memoria flash (Flash-EEPROM), por ejemplo de una memoria flash con una arquitectura

NAND o una arquitectura NOR. Además de una parte regrabable la memoria no volátil 107 puede presentar además una memoria ROM (no representada en la figura 1).

Naturalmente en formas de realización de la invención la tarjeta con chip 101 puede presentar también componentes adicionales o bloques funcionales que no están representados en la figura 1, como por ejemplo un coprocesador criptográfico que puede respaldar como componentes hardware dedicado al procesador 103 en la realización de operaciones criptográficas.

La memoria no volátil 107 de la tarjeta con chip 101 puede estar configurada de modo que esté almacenada en este clave de programa que puede ejecutarse por el procesador 103. Por ejemplo en la memoria no volátil pueden estar almacenados un sistema operativo, aplicaciones y similares. En particular en la memoria no volátil 107 de la tarjeta con chip 101 puede estar implementado una clave de programa, mediante el cual la tarjeta con chip 101 está diseñada para procesar un conjunto de datos 120 que comprende datos útiles encriptados que se transmite a la tarjeta con chip 101 por el servidor o el sistema en segundo plano 111 de modo que se describirá en detalle a continuación en relación con las figuras 2 a 4 adicionales. En el caso de datos útiles encriptados del conjunto de datos 120, que según formas de realización de la invención puede componerse de varios bloques de mensajes, puede tratarse por ejemplo de una actualización de software para la tarjeta con chip 101, en particular para su sistema operativo.

La figura 2 muestra un método 200 para la transferencia segura de datos útiles desde el sistema en segundo plano, en particular servidor, 111 al elemento de seguridad 101 según una forma de realización.

El método 200 comprende la facilitación 201 de una clave de encriptación K_{ENC} y de una clave de valor de comprobación K_{MAC} en el elemento de seguridad 101. En caso de la clave de valor de comprobación K_{MAC} puede tratarse en particular de una clave para la creación de un MAC (*Message Authentication Code*).

El método 200 comprende además la encriptación 203 de los datos útiles mediante la clave de encriptación KENC empleando un cifrado, para generar al menos un primer texto cifrado c1 y un segundo texto cifrado c_2.

Tal como se describe con detalle a continuación, en el caso del cifrado, que se emplea para la encriptación (así como para la desencriptación) de los datos útiles mediante la clave de encriptación KENC, según formas de realización de la invención puede tratarse de un cifrado por bloques y/o de un cifrado en flujo. En el uso de un cifrado por bloques se trata en caso del primer texto cifrado c_1 y el segundo texto cifrado c_2 de un primer bloque de cifras c_1 y de un segundo bloque de cifras c_2.

El método comprende además la transferencia 205 de un conjunto de datos 120 al elemento de seguridad 101, comprendiendo el conjunto de datos transferido completamente 120 el primer texto cifrado c_1, el segundo texto cifrado c_2, un valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación del segundo texto cifrado $h(c_2)$, un valor de comprobación de un primer valor de comprobación basado en claves $h(MAC_1)$, estando incluido en el primer valor de comprobación basado en claves MAC_1 el valor de comprobación del primer texto cifrado $h(c_1)$, un valor de comprobación de un segundo valor de comprobación basado en claves $h(MAC_2)$, estando incluidos en el segundo valor de comprobación basado en claves MAC_2 el primer valor de comprobación basado en claves MAC_1 y el valor de comprobación del segundo texto cifrado $h(c_2)$, así como una firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves $Sign_1[h(c_1)||h(MAC_1)]$.

Tal como se describe en detalle a continuación, en caso de valores de comprobación puede tratarse en particular de valor *de* resumen criptográfico y en el caso de valores de comprobación basados en claves de MAC.

Formas de realización adicionales del método 200, del elemento de seguridad 101 y del sistema en segundo plano, en particular del servidor, 111 se describen a continuación.

Por parte del elemento de seguridad en forma de la tarjeta con chip 101 se genera un par de claves asimétrico con una clave pública PB y una clave privada dB que sirve para la derivación de claves simétricos utilizados en métodos adicionales. En el sistema en segundo plano, en particular servidor, 111 se generan dos pares de claves de firma asimétricos con claves públicos PSA1 y PSA2 y en cada caso claves privados dSA1 y dSA2 correspondientes. El clave privada dB así como los claves de firma públicos PSA1 y PSA2 se almacenan protegidos en la tarjeta con chip 101 frente a manipulación y acceso, por ejemplo en la memoria flash 107 de la tarjeta con chip 101. Estas etapas pueden realizarse en el marco de una personalización de la tarjeta con chip 101 por parte del fabricante de la tarjeta con chip 101.

Según formas de realización de la invención los pares de claves descritos anteriormente pueden generarse por ejemplo mediante curvas elípticas, es decir en caso de los pares de claves dB, PB y dA, PA puede tratarse de pares de claves EC. En este sentido se aplica para PA := dA*G y para PB := dB*G, designando G el punto básico que se compone de la coordenada x Gx y de la coordenada y Gy de la curva elíptica E(F(p)). La curva elíptica está definida por los parámetros de sistema públicos /no públicos, concretamente p, a, b, Gx, Gy, n y el cofactor h. La

multiplicación escalar en el grupo implicado mediante E() se designa con *. La concatenación (en inglés *concatenation*) se representa con ||.

Si la tarjeta con chip 101 se encuentra en uso y resulta que es necesaria una actualización del sistema operativo implementado en la tarjeta con chip 101 según formas de realización de la invención se procede como sigue.

Inicialmente por el sistema en segundo plano, en particular servidor, 111 se genera un par de claves efímeras con clave pública PA y clave privada dA. Además los datos útiles pueden dividirse en una secuencia de n bloques de datos $datos_1$ a $datos_n$. Con ayuda de la clave privada del par de claves efímeras dA y de la clave pública PB, por el sistema en segundo plano, en particular servidor, 111 empleando una función de establecimiento de claves KA(x) se calcula un secreto para derivar mediante una función de derivación de claves KDF(x) a partir de este secreto una clave de encriptación K_{ENC}, una clave para generar códigos de autenticación de mensajes K_{MAC} así como parámetros de inicialización IV_{ENC} y IV_{MAC}. Con un método de encriptación simétrico y la clave de encriptación K_{ENC} a partir de los n bloques de datos se generan después n textos cifrados c_1 a c_n.

KA(x) designa una función para el establecimiento de claves (*Key Agreement*) que empleando una clave privada de una sucesión de bytes x calcula una nueva sucesión de byte que representa un secreto común que el propietario de la clave privada comparte con un socio. Para que el socio pueda calcular igualmente la sucesión de bytes idéntica al socio además de la sucesión de bytes x debe facilitársele un parámetro adicional que le posibilite el cálculo de valor idéntico del secreto (por ejemplo la clave pública del par de claves asimétricas). Las propiedades necesarias de KA(x) son que debe ser prácticamente imposible que (i) mediante conocimiento de la sucesión de bytes x y de la clave pública pueda deducirse la clave privada empleada e (ii) mediante conocimiento de la sucesión de bytes x y de la clave pública pueda deducirse el valor del secreto resultante. Los protocolos de establecimiento de claves habituales, por ejemplo el protocolo de establecimiento de claves de Diffie-Hellman o ECKA en una implementación adecuada reúnen estas propiedades criptográficas y por lo tanto son adecuadas para el uso en formas de realización de la invención. Según formas de realización de la invención la función para el establecimiento de claves puede realizarse mediante una implementación de software que puede recurrir a componentes de hardware dedicados con el fin de llevar a cabo las operaciones básicas matemáticas necesarias para precisión arbitraria, por ejemplo multiplicaciones de números grandes modulares en cuerpos primos, mediante componentes de hardware.

KDF(x) designa una función para la derivación de claves (*Key Derivation*), que empleando la sucesión de bytes x genera una sucesión de bytes de longitud arbitraria. Según formas de realización de la invención a partir de esta sucesión de bytes pueden derivarse las claves K_{ENC} y K_{MAC} así como los vectores de inicialización IV_{ENC} y IV_{MAC} para las funciones $ENOP_k(x)$ y $MAC_k(x)$. Las propiedades necesarias de una función de derivación de claves adecuada según la invención son que (i) prácticamente debe ser imposible imitar la sucesión de bytes generada en el marco de un ataque de fuerza bruta "*Brute Force*", e (ii) se realiza una reproducción determinística de la sucesión de bytes Las funciones de derivación de claves habituales, por ejemplo funciones de derivación de claves basadas en SHAx o basadas en AES, cumplen en el caso de una implementación adecuada estas propiedades criptográficas y por lo tanto son adecuadas para el uso en formas de realización de la invención. Según formas de realización de la invención la función para la derivación de claves puede realizarse mediante una implementación de software, que puede recurrir a componentes de hardware dedicados, para poder permitir realizar las operaciones básicas matemáticas necesarias, por ejemplo AES, mediante componentes de hardware.

A continuación se genera la secuencia de mensajes 120 representada en la figura 1, que se denomina en este caso también conjunto de datos 120, por el sistema en segundo plano, en particular servidor, 111 como sigue, tal como está representado en detalle en la figura 3 en el marco de una forma de realización. El primer mensaje 121 del conjunto de datos 120 se compone de la clave efímera pública PA, un valor *de* resumen criptográfico del primer texto cifrados $h(c_1)$ con $c_1 = ENC(K_{ENC}, IV_{ENC} || datos)$, un valor de resumen criptográfico de un primer códigos de autenticación de mensajes $h(MAC_1)$ con $MAC_1 = MAC(K_{MAC}, IV_{MAC} || c_1)$ del primer texto cifrado, que se genera con la clave K_{MAC}, así como de una firma $Sign_1$ generada con la clave de firma privada dSA1 a través de la clave efímera pública PA, el valor *de* resumen criptográfico del primer texto cifrados $h(c_1)$ así como el valor *de* resumen criptográfico $h(MAC_1)$.

El segundo mensaje hasta el antepenúltimo incluido 123-129 se componen de triples de un texto cifrado c_i con i = 1 ... n-1, un valor *de* resumen criptográfico del texto cifrado siguiente $h(C_{i+1})$ así como un valor de resumen criptográfico de un MAC o código de autenticación de mensajes, que se calcula a través del MAC o código de autenticación de mensajes del texto cifrado actual c_i así como el valor de resumen criptográfico del siguiente texto cifrado, es decir $h(MAC(K_{MAC}, MAC_i || h(c_{i+1}))$.

El penúltimo mensaje 129 se compone del texto cifrado c_n.

El último mensaje 131 se compone de una firma del valor de resumen criptográfico generada con la clave de firma privada dSA2 del MAC o código de autenticación de mensaje a través del último texto cifrado c_n, es decir $h(MAC_n)$.

ENC(K, x) o ENCK(x) designa una función de encriptación que transforma una sucesión de bytes x con ayuda de un algoritmo de encriptación y de una clave simétrica K en un criptograma (*ciphertext* o texto cifrado). Según formas de

realización de realización preferentes de la invención se trata en este sentido de un cifrado en flujo basado en un algoritmo de encriptación por bloques, por ejemplo AES-128. Según formas de realización de la invención el encriptado por bloques puede realizarse mediante un componente de hardware dedicado, por ejemplo mediante un coprocesador criptográfico.

h(x) designa una función de resumen criptográfico (*hash*), que reproduce una sucesión de bytes x de (en teoría) longitud discrecional en una sucesión de bytes de longitud definida, es decir el valor de resumen criptográfico. Las propiedades necesarias de una función resumen adecuada para formas de realización de la invención son que prácticamente debe ser imposible, (i) mediante el conocimiento del valor de resumen criptográfico deducir la sucesión de bytes x y (ii) encontrar al valor de resumen criptográfico de una sucesión de bytes x una segunda sucesión de bytes x' que entregue un valor *de resumen criptográfico* idéntico. Los algoritmos de resumen criptográfico habituales (por ejemplo algoritmos de las familias de funciones de resumen criptográfico SHA2 o SHA3) reúnen en caso de una implementación correcta estas propiedades criptográficas, y por lo tanto son adecuadas para el uso en formas de realización de la invención. Según formas de realización de la invención la función resumen puede realizarse mediante una implementación de software correspondiente o como alternativa mediante un componente de hardware dedicado.

MAC(K, x) o $MAC_K(x)$ designa una función, que a una sucesión de bytes x (de longitud en teoría arbitraria) con ayuda de una clave secreta K calcula un código de autenticación de mensajes (MAC) de longitud definida, que se denomina también valor de resumen criptográfico basado en código. Las propiedades necesarias de una función MAC son que prácticamente debe ser imposible, (i) mediante conocimiento del MAC deducir la clave empleada, (ii) encontrar a un código de autenticación de mensajes de una sucesión de bytes x una segunda sucesión de bytes x' que suministre un código de autenticación de mensajes idéntico, y (iii) sin conocimiento de la clave K calcular a una sucesión de bytes el código de autenticación de mensajes correcto. Los algoritmos MAC habituales, preferiblemente basados en algoritmos de encriptación por bloques, por ejemplo AES-CBC o AES-CMAC, o algoritmos de resumen criptográfico, por ejemplo HMAC, cumplen en el caso de una implementación adecuada estas propiedades criptográficas y por lo tanto son adecuados para el uso en formas de realización de la invención. Según formas de realización de la invención la encriptación por bloques y por lo tanto el cálculo MAC puede realizarse mediante un componente de hardware dedicado.

Sign(x) designa una función de firma que calcula a una sucesión de bytes x con ayuda de la clave privada dSA1 o dSA2 de un par de claves asimétricas calcula una firma criptográfica. La corrección de la firma puede verificarse con ayuda de la clave pública PSA1 o PSA2 del par de claves asimétricas. Las propiedades necesarias de una función de firma son que prácticamente debe ser imposible, (i) deducir mediante conocimiento de la sucesión de bytes x y de la firma la clave privada empleada dSA1 o dSA2, (ii) deducir mediante conocimiento de la clave de verificación pública PSA1 o PSA2 la clave privada empleada dSA1 o dSA2, (iii) encontrar a la firma de una sucesión de bytes x encontrar una segunda sucesión de bytes x' que suministre una firma idéntica, y (iv) sin conocimiento de la clave privada dSA1 o dSA2 calcular a una sucesión de bytes x la firma correcta. Los algoritmos de firma habituales, por ejemplo RSA o ECDSA, reúnen en caso de una implementación correcta estas propiedades criptográficas y por lo tanto son adecuados para el uso en formas de realización de la invención. Según formas de realización de la invención la función de firma Sign(x) puede realizarse mediante una implementación de software, que puede recurrir a componentes de hardware dedicados, para poder permitir realizar las operaciones básicas matemáticas necesarias para precisión arbitraria, como por ejemplo multiplicaciones de números grandes modulares en cuerpos primos, mediante componentes de hardware.

La secuencia de mensajes 120 se transfiere del sistema en segundo plano, en particular servidor, 111 al elemento de seguridad en forma de la tarjeta con chip 101. Tras la obtención del primer mensaje 121 la tarjeta con chip 101 verifica inicialmente la firma sobre los datos transferidos con la clave de firma pública PSA1 almacenada y continúa solo en caso de una comprobación de firma exitosa. Con ayuda de la clave privada dB así como de la clave pública efímera PA se calcula de la tarjeta con chip 101 el secreto común empleando una función de establecimiento de claves, por ejemplo el protocolo de establecimiento de claves de Diffie-Hellman o ECKA, y a partir de ello se deriva la clave de encriptación K_{ENC}, la clave para generar códigos de autenticación de mensajes K_{MAC}, el parámetro de inicialización IV_{ENC} y el parámetro de inicialización IV_{MAC}. Para el segundo hasta el penúltimo mensaje 123-129 la tarjeta con chip 101 comprueba en cada caso, si el valor *de resumen criptográfico*, transferido en el mensaje anterior, del código de autenticación de mensajes del texto cifrado actual coincide realmente con el valor *de resumen criptográfico* calculado del código de autenticación de mensajes del texto cifrado transferido realmente en el mensaje anterior. En el caso de que no se presente ninguna coincidencia, la tarjeta con chip 101 interrumpe el proceso de transferencia. De lo contrario la tarjeta con chip 101 desencripta el texto cifrado con ayuda de la clave derivada K_{ENC} al bloque de datos.

En el último mensaje 131 del conjunto de datos 120 mediante la tarjeta con chip 101 se verifica la firma del valor *de resumen criptográfico* del código de autenticación de mensajes sobre el último texto cifrado con ayuda de la clave de firma pública PSA2. Solo cuando la firma se haya verificado correctamente se siguen empleando los datos útiles $datos_1$ a $datos_n$ encriptados, por ejemplo para actualizar funciones de seguridad del sistema operativo del elemento de seguridad. De lo contrario estos datos son rechazados por la tarjeta con chip 101.

Según formas de realización de realización preferentes de la invención para la encriptación de los bloques de datos útiles se emplean $datos_i$ del estándar AES (*Advanced Encryption Standard*) en el modo OFB, tal como está representado esquemáticamente en la figura 4, en la que bloques de datos útiles se enlazan mediante una operación XOR con una clave que varía. En otras palabras, según formas de realización de la invención en el caso del cifrado, que se emplea para la encriptación de los datos útiles mediante la clave de encriptación K_{ENC} se trata de un cifrado en flujo, que en una parte del método basada en claves genera un flujo de claves, mediante el cual en una parte del método no basada en claves se generan el primer texto cifrado (c_1) y el segundo texto cifrado (c_2).

Por ello se impide que una unidad AES procese datos que se conocen fuera de la tarjeta con chip 101. Para el inicio de la encriptación según formas de realización de la invención se emplea el parámetro de inicialización IV_{ENC} (apartado 401-1 en la figura 4). Para todas las operaciones siguientes se utiliza el bloque de texto cifrado AES, que se empleó para la encriptación del último bloque de datos en el comando anterior, como bloque encadenado (*chaining-block*) (apartados 401-2 a 401-n de la figura 4).

Según formas de realización de la invención los bloques de cifras c_i pueden calcularse de la siguiente manera:

$c_1 := \text{AES-OFB}(K_{ENC}, IV_{ENC} \,||\, datos_1)$
$c_i := \text{AES-OFB}(K_{ENC}, datos_i)$; con i = 2, 3, ..., n,

refiriéndose AES-OFB al "*Advanced Encryption Standard*" en el modo "*Output Feedback*" (retroalimentación de salida).

Según formas de realización de la invención los códigos de autenticación de mensajes MAC_i pueden calcularse de la siguiente manera:

$MAC_1 := \text{AES-CMAC}(K_{MAC}, IV_{MAC} \,||\, h(c_1))$
$MAC_i := \text{AES-CMAC}(K_{MAC}, MAC_{i-1} \,||\, h(c_i))$; con i := 2, 3, ..., n,

refiriéndose AES-CMAC a "*Cipher-based Message Authentication Code*" (código de autenticación de mensajes basado en cifrado) empleando el estándar "*Advanced Encryption Standard*". Por lo tanto según formas de realización de la invención tanto para la encriptación como para el cálculo de los códigos de autenticación de mensajes puede utilizarse ventajosamente una unidad AES.

Según formas de realización de la invención, las firmas anteriormente descritas se basan en curvas elípticas. Por ejemplo las firmas pueden calcularse de la siguiente manera:

$Sign_1 := \text{ECDSA}[dSA1, h(PA.x \,||\, h(c_1) \,||\, h(MAC_1)]$
$Sign_2 := \text{ECDSA}[dSA2, h(MAC_n)]$,

refiriéndose ECDSA a "*Elliptic Curve Digital Signature Algorithm*" (algoritmo de firma digital de curva elíptica).

Por razones de rendimiento en caso de formas de realización del elemento de seguridad de acuerdo con la invención en forma la tarjeta con chip 101 pueden realizarse las rutinas de encriptación y desencriptación criptográficas anteriormente descritas así como las rutinas anteriormente descritas para el cálculo de códigos de autenticación de mensajes en hardware, por ejemplo empleando un coprocesador criptográfico. Dado que para el cálculo se emplea material de clave secreto (en la presente memoria: las claves derivadas K_{ENC} y K_{MAC}) según formas de realización de la invención la utilidad de tales rutinas se minimiza mediante un atacante por medio de la transferencia de datos modificados - en particular antes de garantizar la autenticidad de los datos transferidos, para generar lo menos posible fenómenos observables física o lógicamente. Las formas de realización de la invención presentan varias propiedades que pueden limitar al mínimo un uso tal de rutinas tal como se describe detalladamente a continuación.

Según formas de realización de la invención la desencriptación de datos se realiza exclusivamente tras garantizar la autenticidad de los datos transferidos. Técnicamente esto sucede en formas de realización de la invención mediante la comprobación de la firma y del código de autenticación de mensajes en el primer mensaje averiguado 121 antes de que se descodifique el primer texto cifrado c_1 que es parte del mensaje 123. Mediante el encadenamiento de códigos de autenticación de mensajes (el código MAC_i está incluido en el código MAC_{i+1}) también para los bloques de sucesión de los mensajes adicionales queda garantizado que se descodifiquen exclusivamente bloques de datos autentificados. Esto minimiza la posibilidad de que un atacante mediante la observación de la tarjeta con chip 101 durante un proceso de desencriptación de bloques de datos preparados puedan obtenerse informaciones físicas o lógicas utilizables, siempre que él no posea la clave de firma secreta dSA1 y dSA2. Sin embargo estas no están almacenadas en la tarjeta con chip 101, sino en el sistema en segundo plano, en particular, servidor 111. Mediante el mantenimiento en secreto adicional de los parámetros de sistema, que se utilizan en el marco del método de firma, como por ejemplo parámetros de una curva elíptica empleada para el método de firma se descartan ataques matemáticos en el método criptográfico asimétrico empleado, de modo que el cálculo de dSA1 o dSA2 a partir de PSA1 o PSA2 no es posible. Dado que los parámetros de sistema exclusivamente tienen que ser conocidos por el

fabricante o el creador de los datos útiles no es necesaria una distribución. Además en la tarjeta con chip 101 están presentes varios conjuntos de parámetros de sistema, y se emplean para distintas actualizaciones. La referencia del conjunto de parámetros de sistema empleados puede ser en este caso parte de la clave pública PSA1 o PSA2.

Según formas de realización de la invención los valores *de resumen criptográfico* de los bloques de cifras sirven como entrada para el cálculo de los códigos de autenticación de mensajes. Las funciones resumen criptográficas reproducen los bloques de cifras, potencialmente grandes, en una sucesión de signos con longitud reducida, fija. El cálculo de los códigos de autenticación de mensajes se realiza solo en esta sucesión de signos corta. Por ello la utilización de la rutina para el cálculo del código de autenticación de mensajes se limita al mínimo, de modo que pueden producirse fenómenos observables solo durante un espacio de tiempo reducido.

Según formas de realización de la invención en el cálculo de los códigos de autenticación de mensajes está incluida la clave secreta K_{MAC}. Para evitar que un atacante mediante el conocimiento de varios códigos de autenticación de mensajes pueda extraer conclusiones sobre la clave secreta K_{MAC}, los parámetros para generar la clave secretan o el secreto calculado común que sirve de base el método posee según formas de realización de la invención la propiedad de que se transmiten valores *de resumen criptográfico* de los códigos de autenticación de mensajes como parte de los mensajes del conjunto de datos 120. Mediante el método asimétrico de la derivación de la clave K_{MAC} común y secreta el cálculo del código de autenticación de mensajes puede realizarse exclusivamente sobre la tarjeta con chip 101. Por lo tanto la transferencia del código de autenticación de mensajes a la tarjeta con chip 101 no es necesaria; la transferencia de los valores *de resumen criptográfico* criptográficos es suficiente. Un atacante por tanto incluso al obtener el conocimiento de la secuencia de mensajes no posee ningún conocimiento de los códigos de autenticación de mensajes.

Para evitar que un atacante mediante el conocimiento de varios bloques de datos útiles pueda sacar conclusiones de la clave secreta K_{MAC} y/o los parámetros para generar la clave secreta o el secreto común calculado tomado como base, el método según formas de realización de la invención posee la propiedad de que se anticipe un bloque de datos desconocido para el cálculo del código de autenticación de mensajes. Ya que según formas de realización de la invención a los datos de entrada para el cálculo del código de autenticación de mensajes MAC_{i+1} se anticipa el código de autenticación de mensajes MAC_i desconocido fuera de la tarjeta con chip 101. Todos los demás bloques de datos se enlazan en caso de una selección adecuada de la función de enlace (por ejemplo modo CBC) con el resultado intermedio del bloque de datos precedente en cada caso. Para el primer código de autenticación de mensajes se anticipa el valor IV_{MAC} que puede calcularse junto con la clave K_{MAC} a partir del secreto común.

Según formas de realización de la invención en el cálculo de los bloques de mensajes está incluida la clave secreta K_{ENC}. Para evitar que un atacante mediante del conocimiento de varios bloques de cifras pueda sacar conclusiones sobre la clave secreta K_{ENC} y/o los parámetros para generar la clave secreta o el secreto común calculado tomado como base, el método según formas de realización de la invención posee la propiedad de que pueda evitarse un método basado en claves para generar los bloques de cifras en los mensajes. Mediante el método asimétrico de la derivación del secreto común y con ello de la clave secreta K_{ENC} el método de desencriptación puede exclusivamente realizarse exclusivamente en el entorno seguro de la tarjeta con chip 101. Según formas de realización de la invención el método de desencriptación está seleccionado de modo que está compuesto de una parte basada en claves y una parte no basada en claves, procesándose directamente el texto cifrado conocido externamente solo mediante la parte no basada en claves del método. Esta configuración puede garantizar que un atacante para el análisis de fenómenos observables física o lógicamente que están correlacionados con la clave K_{ENC}, no pueda emplear datos conocidos fuera de la tarjeta con chip 101.

Existe el peligro de que un atacante consiga la posesión de una tarjeta con chip 101 y pueda la utilizar para leer la clave privada dB depositada por ejemplo en la memoria flash 107, por ejemplo mediante fenómenos observables física o lógicamente. Con el conocimiento de la clave dB el atacante puede derivar las claves K_{ENC} y K_{MAC} y con ello encriptar datos discrecionales y falsificar códigos de autenticación de mensajes. Mediante la siguiente propiedad de formas de realización de la invención el atacante no obstante no puede reproducir datos útiles falsificados. En el caso de que un atacante sustituya en un lugar discrecional el texto cifrado c_i por un texto cifrado c_i' falsificado. Para que el texto cifrado falsificado c_i' se reconozca como auténtico por la tarjeta con chip 101, según formas de realización de la invención también el código de autenticación de mensajes correspondiente $MAC_i = MAC(K_{MAC}, MAC_{i-1} \,||\, h(C_i))$ tiene que ser correcto. Según formas de realización de la invención el valor calculado MAC_i sin embargo sirve a su vez como entrada para el código de autenticación de mensajes siguiente MAC_{i+1}, de modo que también el atacante debe crear como nuevo este código de autenticación de mensajes hasta el último código de autenticación de mensajes. Sin embargo este está provisto con una firma, de modo que la tarjeta con chip 101 detecta como muy tarde en este punto que el texto cifrado c_i mediante se ha sustituido por un texto cifrado C_i' falsificado.

Según formas de realización de la invención el carácter confidencial de los datos útiles se produce continuamente tras la creación de la secuencia de mensajes 120. Esto se garantiza según formas de realización de la invención porque los datos útiles se encriptan con ayuda de una clave simétrica derivada K_{ENC}. Un atacante puede solo con conocimiento de la clave secreta dB (que está almacenada en la tarjeta con chip 101 protegida contra el acceso) o conocimiento de la clave secreta dA (mantenida en secreto mediante la creación de la secuencia de mensajes 120)

desencriptar de nuevo los datos útiles encriptados. Los parámetros de sistema (por ejemplo mediante el empleo de curvas elípticas los parámetros de curvas) necesarios para el método de establecimiento de claves pueden mantenerse en secreto adicionalmente. En particular una extracción de la clave secreta dB con ayuda de fenómenos observables física o lógicamente se ve dificultada de manera significativa mediante un conjunto de parámetros de sistema desconocido dado que los análisis matemáticos necesarios condicionan el conocimiento de parámetros de sistema. Además incluso con una extracción exitosa de dB sin conocimiento de los parámetros de sistema el cálculo del secreto común y como consecuencia el cálculo de K_{ENC} y K_{MAC} no es posible. Además se descartan ataques matemáticos en el método criptográfico asimétrico empleado, de modo que el cálculo de dA a partir de no es posible. Dado que los parámetros de sistema deben ser conocidos exclusivamente por el fabricante de la tarjeta con chip 101 o el proveedor de los datos útiles no es necesaria una distribución. Además según formas de realización de la invención en la tarjeta con chip 101 pueden estar depositados varios conjuntos de parámetros de sistema y emplearse para la reproducción reiterada de datos útiles. Según formas de realización de la invención en este caso un identificador que identifique el conjunto de parámetros de sistema que va a emplearse por ejemplo puede ser parte de la clave pública PA.

Las formas de realización de la invención gracias al tipo de la garantía del carácter confidencial de los datos útiles presentan además la siguiente propiedad. Dado que el carácter confidencial de los datos útiles también se da en el caso de conocimiento de la secuencia de mensajes 120 los datos útiles también pueden usarse, por ejemplo instalarse sin conocimiento de las claves secretas por parte de terceros.

Las formas de realización de la invención pueden utilizarse ventajosamente en caso de elementos de seguridad que no disponen de capacidad de almacenamiento suficiente con el fin de almacenar el texto cifrado en su totalidad en conjunto y desencriptar en el elemento de seguridad. Además pueden utilizarse formas de realización de la invención en caso de elementos de seguridad, en los que no es posible realizar al mismo tiempo un código de determinadas zonas de almacenamiento (prueba de autenticidad, desencriptado y al mismo tiempo leer datos de esta zona de almacenamiento y grabarlos allí. En particular la división del conjunto de datos 120 en varios mensajes o bloques de mensajes según formas de realización de la invención posibilita un aprovechamiento en elementos de seguridad con recursos limitados. Esto posibilita comprobar para cada bloque de mensajes inicialmente la autenticidad del texto cifrado del bloque de mensajes y tras la comprobación desencriptar los datos útiles y depositarlos en una memoria del elemento de seguridad en forma de la tarjeta con chip 101. Según formas de realización de la invención no existe por tanto ninguna necesidad de depositar todo el texto cifrado en conjunto en la memoria 107 de la tarjeta con chip 101. Mediante el tamaño reducido seleccionable de los bloques de cifras individuales más pequeños pueden realizarse prueba de autenticidad y desencriptación en la memoria aleatoria.

Las formas de realización de la invención necesitan como máximo dos comprobaciones de firma, concretamente de la firma en el primer bloque de mensajes 121 y de la firma en el último bloque de mensajes 131, y por lo tanto presentan un alto rendimiento, lo que es ventajoso en particular en caso de elementos de seguridad con reducida capacidad de cómputo.

Las formas de realización de la invención consideran la capacidad de comunicación posiblemente limitada de elementos de seguridad, distribuyéndose cantidades de datos mayores de una operación de actualización en varios mensajes. En este sentido la granularidad en la que se descomponen las cantidades de datos puede ajustarse a escala de manera arbitraria y depende principalmente solo de la capacidad de la interfaz de comunicación del elemento de seguridad.

Tal como ya se ha descrito anteriormente, en la figura 3 se ilustra cómo pueden realizarse según formas de realización de la invención la descomposición de todos los datos útiles 120 en unidades más pequeñas $datos_1$, $datos_2$ ... $datos_n$. Las formas de realización de la invención garantizan que todos los mensajes de la para todos los mensajes quede garantizada la protección de autenticidad. Para ello según formas de realización de la invención con ayuda de una función de establecimiento de claves KA(x) en combinación con la derivación de claves KDF(x) se averiguan los parámetros de sistema K_{ENC}, K_{MAC}, IV_{ENC} y IV_{MAC} necesarios para la seguridad simétrica $ENC_K(x)/MAC_K(x)$ de los datos de actualización.

En la figura 3 mediante el mensaje 121 se representa que inicialmente se transmiten los valores para las KA(x)/KDF(x) en forma de PA así como los valores de entrada para la función $Sign_1(x)$ a la tarjeta con chip 101. La firma $Sign_1(x)$ garantiza la integridad y la autenticidad de los valores de entrada. Una manipulación posterior de PA, $h(c_1)$ o $h(MAC_1)$ puede detectarse por lo tanto de manera fiable. Según formas de realización de la invención se transmiten por lo tanto inicialmente los valores de entrada anteriormente mencionados. Tal como muestra la figura 3 además en el cálculo de $MAC_K(x)$ y en la firma final $Sign_2(x)$ los valores MAC de las funciones anteriores $MAC_K(x)$. Por ello queda garantizada una autenticidad e integridad continuas hasta el último bloque de mensajes 131.

En la etapa siguiente se realiza la comprobación de la corrección de los valores *de resumen criptográfico* a través de los bloques de cifras. El empleo de valores *de resumen criptográfico* en la comprobación de MAC tiene dos ventajas. Por un lado el valor de MAC mismo no tiene que desvelarse. Por otro lado para un atacante mediante el cálculo de MAC a través de los valores *de resumen criptográfico* solo hay disponible una cantidad muy reducida de datos aprovechables. En el cálculo del MAC no se emplea el valor *de resumen criptográfico* mismo como entrada en el

cálculo de MAC, sino que se anticipa al valor *de resumen criptográfico* el CMAC o CBC-MAC de la comprobación de MAC anterior, por lo que ambos bloques están enlazados o encadenados entre sí. El enlace, que se realiza en formas de realización de la invención empleando el modo *Block-Chaining* de encadenamiento de bloques lleva a que el bloque de entrada en la operación basada en claves (encriptado por bloques AES) del cálculo de MAC no se conozca. Después de que se haya realizado con éxito la comprobación de MAC mediante una nueva comprobación de valores *de resumen criptográfico* queda garantizada la integridad del texto cifrado. Tras la comprobación exitosa del valor *de resumen criptográfico* se desencriptan los bloques de cifras. Para la desencriptación de los bloques de cifras según formas de realización de la invención se utiliza un cifrado por bloques y/o cifrado en flujo. El flujo de claves puede generarse en este sentido por ejemplo mediante un algoritmo de bloque en el modo OFB o un modo de contador (modo CTR), de modo que no están datos de entrada disponibles de manera externa en la operación de la encriptación basada en claves. Antes de que se acepten todos los datos de actualización encadenados como actualización permitida del sistema operativo mediante el elemento de seguridad se realiza la comprobación de la firma final.

REIVINDICACIONES

1. Método (200) para la transferencia segura de datos útiles a un elemento de seguridad (101), comprendiendo el método (200):

la facilitación (201) de una clave de encriptación (K_{ENC}) y de una clave de valor de comprobación (K_{MAC}) en el elemento de seguridad (101);
la encriptación (203) de los datos útiles mediante la clave de encriptación (K_{ENC}) empleando un cifrado, para generar al menos un primer texto cifrado (c_1) y un segundo texto cifrado (c_2);
la transferencia (205) de un conjunto de datos (120) al elemento de seguridad (101), comprendiendo el conjunto de datos transferido completamente (120) el primer texto cifrado (c_1), el segundo texto cifrado (c_2), un valor de comprobación del primer texto cifrado ($h(c_1)$), un valor de comprobación del segundo texto cifrado ($h(c_2)$), un valor de comprobación de un primer valor de comprobación basado en claves ($h(MAC_1)$), estando incluido en el primer valor de comprobación basado en claves (MAC_1) el valor de comprobación del primer texto cifrado ($h(c_1)$), un valor de comprobación de un segundo valor de comprobación basado en claves ($h(MAC_2)$), estando incluidos en el segundo valor de comprobación basado en claves (MAC_2) el primer valor de comprobación basado en claves (MAC_1) y el valor de comprobación del segundo texto cifrado ($h(c_2)$), así como una firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves ($Sign_1[h(c_1)||h(MAC_1)]$).

2. Método según la reivindicación 1, estando incluido en el primer valor de comprobación basado en claves (MAC_1) además un parámetro de inicialización (IV_{MAC}).

3. Método según la reivindicación 1 o 2, transfiriéndose en la etapa (205) de la transferencia del conjunto de datos (120) al elemento de seguridad (101) un primer mensaje (121), que comprende el valor de comprobación del primer texto cifrado ($h(c_1)$) y el valor de comprobación del primer valor de comprobación basado en claves ($h(MAC_1)$), y transfiriéndose un segundo mensaje (123), que comprende el valor de comprobación del segundo texto cifrado ($h(c_2)$) y el valor de comprobación del segundo valor de comprobación basado en claves ($h(MAC_2)$), al elemento de seguridad (101).

4. Método según la reivindicación 3, comprendiendo el primer mensaje (121) además la firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves $Sign_1[h(c_1)||h(MAC_1)]$.

5. Método según la reivindicación 4, comprendiendo el método las etapas adicionales de, como respuesta a la transferencia del primer mensaje (121) al elemento de seguridad (101) se comprueba la firma sobre del valor de comprobación del primer texto cifrado ($h(c_1)$) y el valor de comprobación del primer valor de comprobación basado en claves ($h(MAC_1)$) del elemento de seguridad (101) y, en caso de que la firma del elemento de seguridad (101) no pueda verificarse, el elemento de seguridad (101) interrumpe el proceso.

6. Método según una de las reivindicaciones 3 a 5, comprendiendo el segundo mensaje (123) además el primer texto cifrado (c_1).

7. Método según una de las reivindicaciones anteriores, comprendiendo el conjunto de datos (120) además una firma sobre del valor de comprobación del segundo valor de comprobación basado en claves $Sign_2[h(MAC_2)]$.

8. Método según la reivindicación 7, transfiriéndose en la etapa (205) de la transferencia del conjunto de datos (120) al elemento de seguridad (101) un mensaje adicional (131) al elemento de seguridad (101), que comprende la firma sobre del valor de comprobación del segundo valor de comprobación basado en claves $Sign_2[h(MAC_2)]$.

9. Método según una de las reivindicaciones anteriores, tratándose en caso del valor de comprobación del primer texto cifrado (h(c1)) de un valor de resumen criptográfico (*hash*) del primer texto cifrado ($h(c_1)$) y en caso del valor de comprobación del segundo texto cifrado ($h(c_2)$) de un valor de resumen criptográfico del segundo texto cifrado ($h(c_2)$).

10. Método según una de las reivindicaciones anteriores, tratándose en el caso del cifrado, que se emplea para la encriptación de los datos útiles mediante la clave de encriptación (K_{ENC}), de un cifrado en flujo que, en una parte basada en claves del método, genera un flujo de claves, mediante el cual en una parte del método no basada en claves se generan el primer texto cifrado (c_1) y el segundo texto cifrado (c_2).

11. Método según la reivindicación 10, tratándose en el caso del cifrado, que se emplea para la encriptación de los datos útiles mediante la clave de encriptación (K_{ENC}), de un cifrado por bloques AES, en particular un cifrado por bloques AES en el modo OFB o modo CTR, o de un cifrado por bloques TDES.

12. Método según la reivindicación 11, siendo el primer valor de comprobación basado en claves y el segundo valor de comprobación basado en claves un MAC, en particular un CMAC o CBC-MAC, y calculándose empleando el

cifrado por bloques AES o el cifrado por bloques TDES.

13. Método según una de las reivindicaciones 1 a 9, empleándose para la encriptación de los datos útiles mediante la clave de encriptación (K_{ENC}) y para la creación de los valores de comprobación basados en claves un cifrado por bloques AES en el modo Galois/CTR.

14. Método según una de las reivindicaciones anteriores, comprendiendo la facilitación (201) de la clave de encriptación (K_{ENC}) y de la clave de valor de comprobación (K_{MAC}) en el elemento de seguridad (101) la etapa del cálculo de un secreto y la etapa de la derivación de la clave de encriptación (K_{ENC}) y de la clave de valor de comprobación (K_{MAC}) a partir del secreto calculado.

15. Método según la reivindicación 14, comprendiendo el conjunto de datos (120) además una clave pública de un par de claves efímeras (PA) y comprendiendo la etapa del cálculo de un secreto el cálculo del secreto basándose en la clave pública del par de claves efímeras (PA) y de una clave (dB) privada depositada de manera segura en el elemento de seguridad (101).

16. Método según la reivindicación 15, comprendiendo el conjunto de datos (120) además una firma sobre de la clave pública del par de claves efímeras (PA) o de una parte de la misma.

17. Elemento de seguridad (101) con:

una interfaz de comunicación (105), que está configurada para recibir un conjunto de datos (120) transferido de un sistema en segundo plano (111), comprendiendo el conjunto de datos (120) transferido completamente un primer texto cifrado (c_1), un segundo texto cifrado (c_2), un valor de comprobación del primer texto cifrado ($h(c_1)$), un valor de comprobación del segundo texto cifrado ($h(c_2)$), un valor de comprobación de un primer valor de comprobación basado en claves ($h(MAC_1)$), estando incluido en el primer valor de comprobación basado en claves (MAC_1) el valor de comprobación del primer texto cifrado ($h(c_1)$), un valor de comprobación de un segundo valor de comprobación basado en claves ($h(MAC_2)$), estando incluidos en el segundo valor de comprobación basado en claves (MAC_2) el primer valor de comprobación basado en claves (MAC_1) y el valor de comprobación del segundo texto cifrado ($h(c_2)$), así como una firma sobre del valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves ($Sign_1[h(c_1)||h(MAC_1)]$); y
un procesador (103), que está configurado para verificar basándose en una clave de encriptación (K_{ENC}) y en una clave de valor de comprobación (K_{MAC}) el conjunto de datos (120) y desencriptar el primer texto cifrado (c_1) y el segundo texto cifrado (c_2).

18. Sistema en segundo plano, en particular servidor, (111) con:

un procesador, que está configurado para encriptar datos útiles mediante una clave de encriptación (K_{ENC}) empleando un cifrado, para obtener al menos un primer texto cifrado (c_1) y un segundo texto cifrado (c_2) y
una interfaz de comunicación (113), que está configurada para transferir un conjunto de datos (120) a un elemento de seguridad (101), comprendiendo el conjunto de datos transferido completamente (120) el primer texto cifrado (c_1), el segundo texto cifrado (c_2) un valor de comprobación del primer texto cifrado ($h(c_1)$), un valor de comprobación del segundo texto cifrado ($h(c_2)$), un valor de comprobación de un primer valor de comprobación basado en claves ($h(MAC_1)$), estando incluido en el primer valor de comprobación basado en claves (MAC_1) el valor de comprobación del primer texto cifrado ($h(c_1)$), un valor de comprobación de un segundo valor de comprobación basado en claves ($h(MAC_2)$), estando incluidos en el segundo valor de comprobación basado en claves (MAC_2) el primer valor de comprobación basado en claves (MAC_1) y el valor de comprobación del segundo texto cifrado ($h(c_2)$), así como una firma sobre el valor de comprobación del primer texto cifrado y el valor de comprobación del primer valor de comprobación basado en claves ($Sign_1[h(c_1)||h(MAC_1)]$).

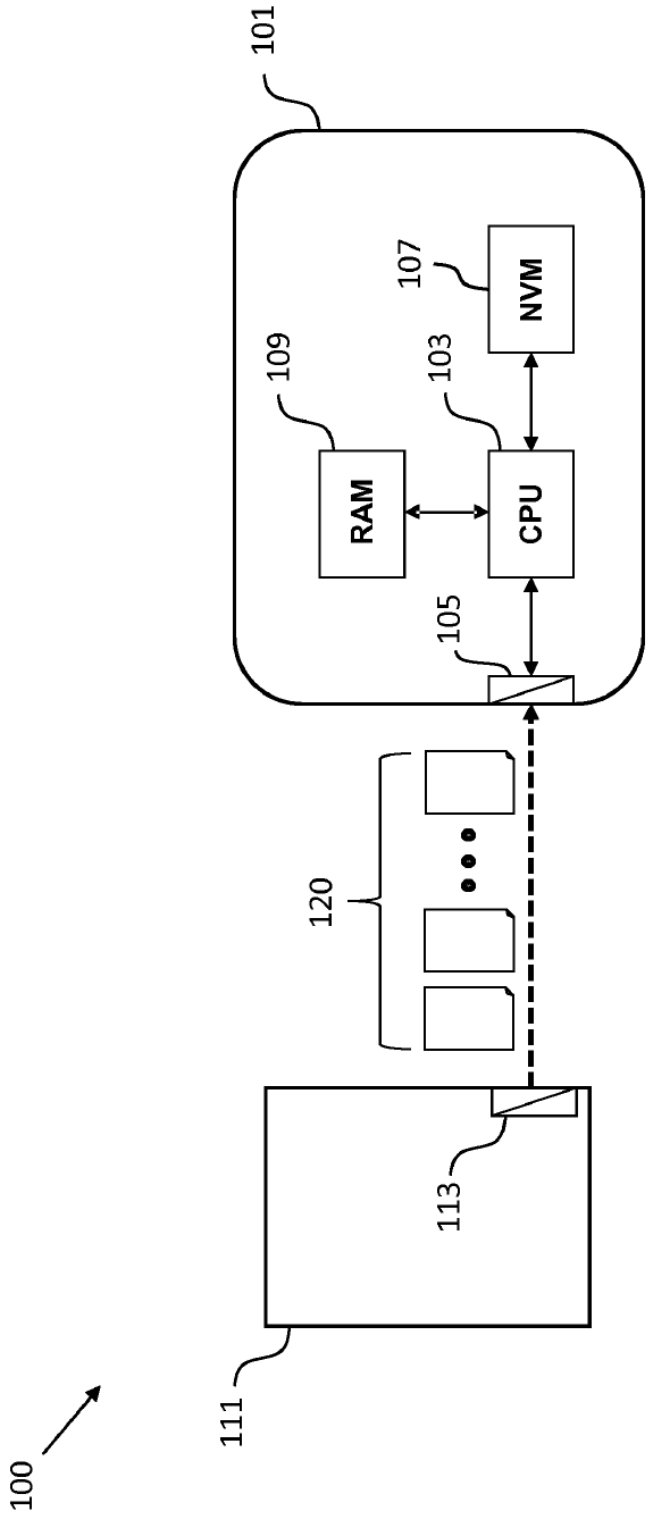

Fig. 1

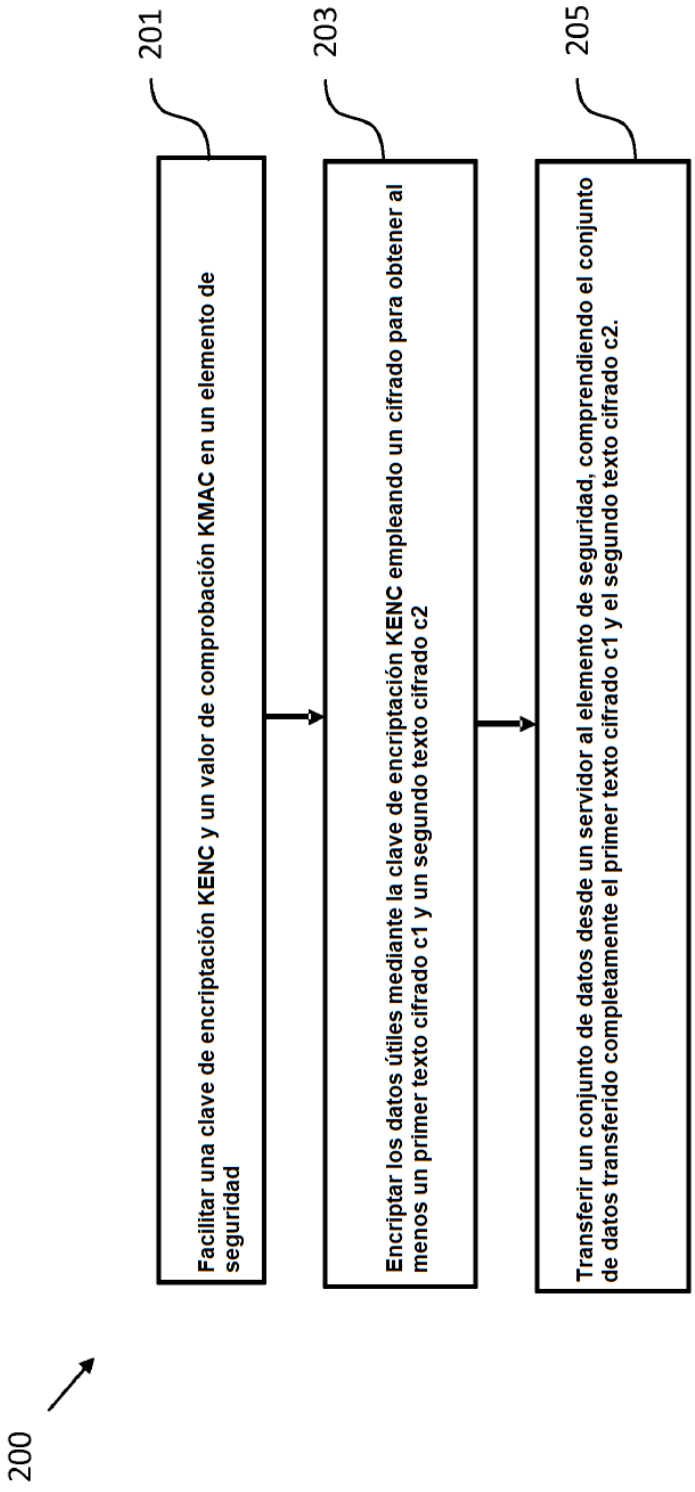
200
201
Facilitar una clave de encriptación KENC y un valor de comprobación KMAC en un elemento de seguridad
203
Encriptar los datos útiles mediante la clave de encriptación KENC empleando un cifrado para obtener al menos un primer texto cifrado c1 y un segundo texto cifrado c2
205
Transferir un conjunto de datos desde un servidor al elemento de seguridad, comprendiendo el conjunto de datos transferido completamente el primer texto cifrado c1 y el segundo texto cifrado c2.

Fig. 2

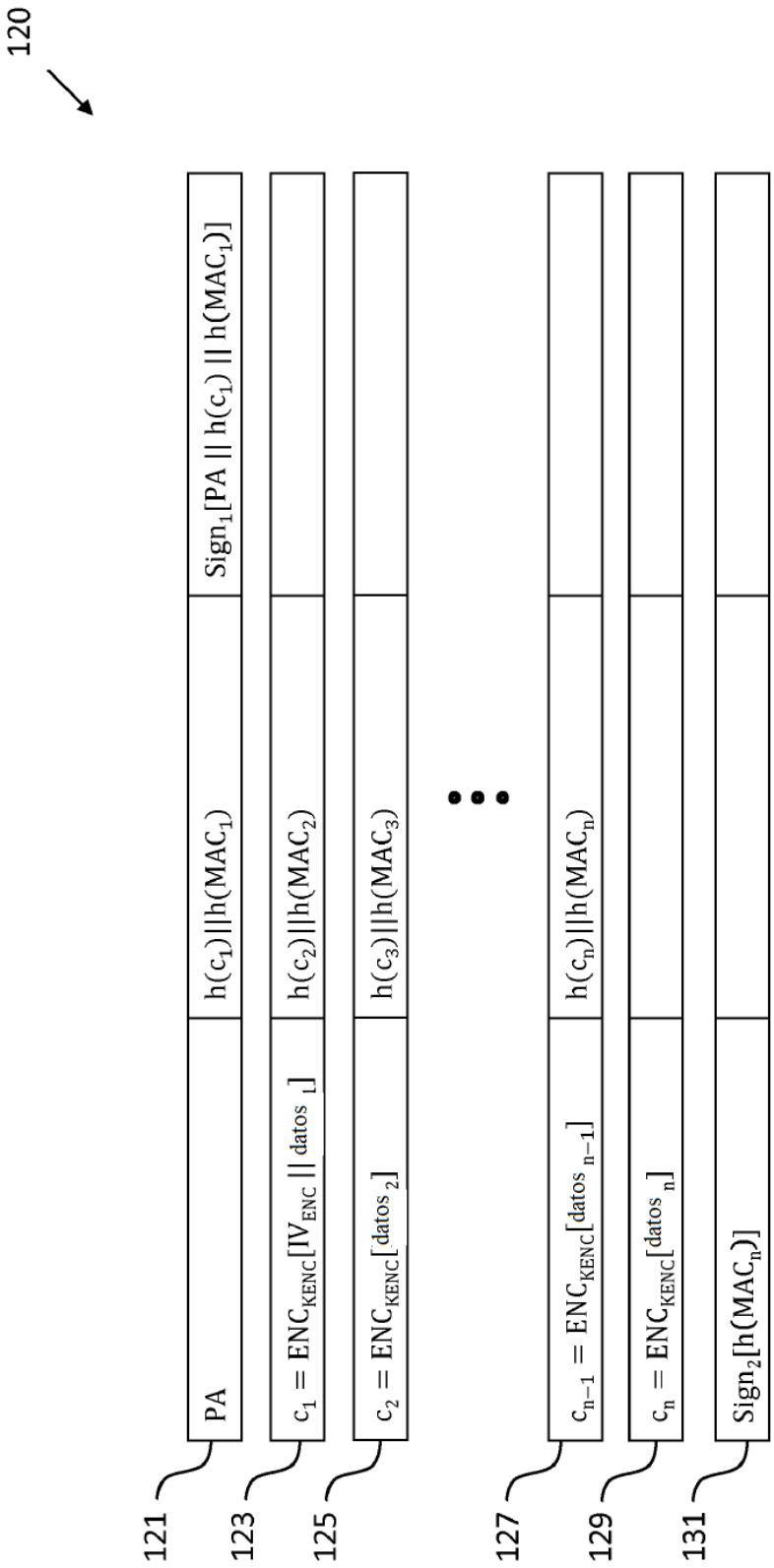
120
121
123
125
127
129
131
PA
$h(c_1)||h(MAC_1)$
$Sign_1[PA || h(c_1) || h(MAC_1)]$
$c_1 = ENC_{KENC}[IV_{ENC} || datos_1]$
$h(c_2)||h(MAC_2)$
$c_2 = ENC_{KENC}[datos_2]$
$h(c_3)||h(MAC_3)$
$c_{n-1} = ENC_{KENC}[datos_{n-1}]$
$h(c_n)||h(MAC_n)$
$c_n = ENC_{KENC}[datos_n]$
$Sign_2[h(MAC_n)]$

Fig. 3

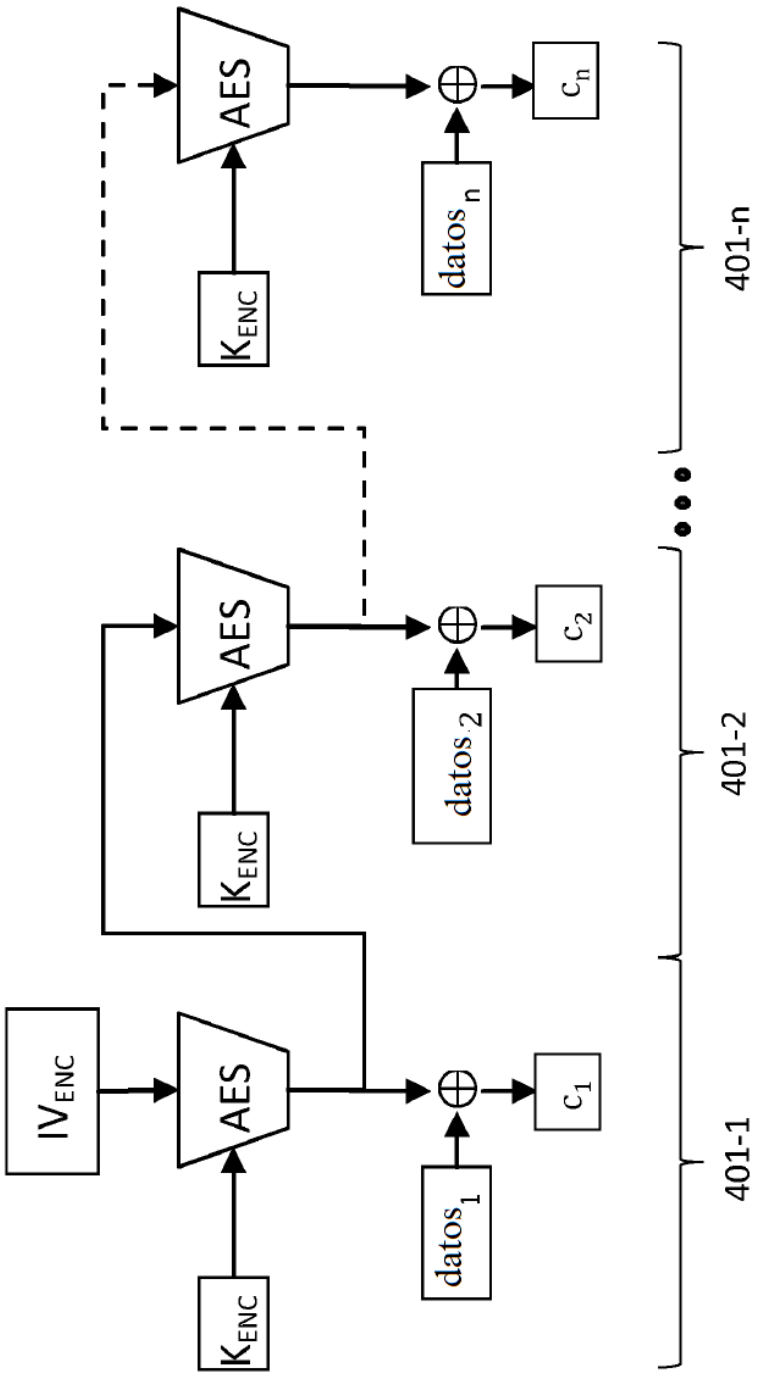
IV_ENC
AES
AES
AES
K_ENC
K_ENC
K_ENC
datos_1
datos_2
datos_n
c_1
c_2
c_n
401-1
401-2
401-n

Fig. 4