(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 805 423**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.03.2017 PCT/EP2017/055244**

(87) Fecha y número de publicación internacional: **28.09.2017 WO17162424**

(96) Fecha de presentación y número de la solicitud europea: **07.03.2017 E 17710849 (5)**

(97) Fecha y número de publicación de la concesión europea: **01.07.2020 EP 3403214**

(54) Título: **Procedimiento y dispositivo para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato**

(30) Prioridad:

22.03.2016 DE 102016204684

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.02.2021

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

MERLI, DOMINIK;
FALK, RAINER y
PYKA, STEFAN

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Procedimiento y dispositivo para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato

La presente invención se refiere a un procedimiento y a un dispositivo para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato, así como a un (producto de) programa informático correspondiente.

Antecedentes de la invención

Hoy en día, en todas ramas de la industria pueden encontrarse aparatos, por ejemplo, sistemas incrustados (en inglés: *Embedded Systems*). La protección (criptográfica) de estos aparatos juega un papel cada vez más importante para poder garantizar un funcionamiento seguro. Mediante funciones criptográficas pueden conseguirse fines como la integridad, la confidencialidad o la autenticidad de estas plataformas. De esta manera, se rechazan ataques intencionados, focalizados.

Una posibilidad para proteger un sistema incrustado es la integración de un anclaje de veracidad basado en hardware. El mismo puede cumplir diversos objetivos, por ejemplo, puede poner a disposición una función de seguridad de una aplicación de seguridad durante el plazo de vigencia de la clave criptográfica, crear y comprobar valores de comprobación de integridad de datos de aplicación y configuración, firmar datos, proporcionar números aleatorios seguros desde el punto de vista criptográfico, y mucho más.

Por tanto, la designación “*anchor*” (en español: anclaje) se debe a que los conceptos de confianza o de seguridad de las instalaciones de procesamiento de datos utilizan el *trust anchor* (anclaje de veracidad) como base y a este respecto se requiere o debe requerirse que el *trust anchor* sea seguro en sí mismo y no esté comprometido.

Un posible *trust anchor* es, por ejemplo, el Trusted Platform Module (TPM, Módulo de plataforma segura) especificado en el año 2009 por la norma ISO/IEC 11889, que está presente en cada PC moderno y se requiere obligatoriamente en los sistemas operativos modernos para determinadas operaciones criptográficas. Por ejemplo, el cifrado de discos duros “BitLocker” del sistema operativo muy difundido “Windows” se basa en un TPM. Por ejemplo, un *trust anchor* también puede realizarse mediante un criptocontrolador, mediante un denominado *secure element* (en español: elemento seguro, por ejemplo, un dispositivo semiconductor de autenticación) o en firmware.

Según la figura 1 es concebible el siguiente escenario con un anclaje de veracidad. Un sistema incrustado ES, por ejemplo, un aparato o un ordenador de control, comprende al menos una aplicación A. El sistema ES también comprende normalmente un sistema operativo no representado en la figura como, por ejemplo, VxWorks, FreeRTOS, Linux o Microsoft Windows. Igualmente no representado en la figura, el aparato presenta por regla general una unidad de control CPU y proporciona una interfaz de USB que está conectada con un puerto USB accesible externamente del aparato. En un módulo de memoria de USB enchufado (o tarjeta SD) pueden estar depositados datos de configuración, por ejemplo, de forma cifrada. Además, el aparato puede disponer de memoria de programa (flash) y memoria volátil (RAM), una interfaz de red (por ejemplo, Ethernet) y una unidad de entrada y salida (E/S) a la que pueden conectarse periféricos (sensores, accionadores). Además, puede estar previsto un *secure element* como anclaje de veracidad.

Las denominadas *apps* o aplicaciones (aplicación) pueden hacer peticiones al *secure element* para que el mismo compute funciones criptográficas. A este respecto, puede tratarse, por ejemplo, de una aplicación de control o una aplicación de diagnóstico. La misma se comunica mediante un dispositivo E o mediante un controlador o un módulo de *kernel* con un anclaje de veracidad V del sistema ES. El dispositivo E se comunica con un anclaje de veracidad V. Una aplicación A establece, por ejemplo, una conexión de comunicación protegida criptográficamente, por ejemplo, mediante una red de comunicación cableada y/o inalámbrica, por ejemplo, WLAN, Ethernet, etc., o quiere descifrar datos de configuración. Para ejecutar esta función segura, la aplicación A solicita una función de seguridad criptográfica, por ejemplo, una clave, una derivación de clave o un cómputo de firma. Se transmite opcionalmente al anclaje de veracidad un parámetro de seguridad SP que puede predefinirse por la aplicación A, por ejemplo, un parámetro de derivación de clave o un parámetro de identificación de clave. Luego, el dispositivo E obtiene del anclaje de veracidad V una función de seguridad criptográfica K, por ejemplo, en forma de una clave derivada dependiendo del parámetro de seguridad SP o fija, que se pasa a la aplicación para proteger la conexión de comunicación.

Sin embargo, si una aplicación de atacante se ha hecho con el aparato o el dispositivo en funcionamiento, puede hacer de manera dinámica peticiones al anclaje de veracidad, que luego ejecuta cualquier operación criptográfica o función de seguridad para la misma. Esto puede mermar claramente la seguridad del aparato.

Por el documento EP 1 102 153 A2 se conoce además un procedimiento y un sistema con el que pueden construirse implementaciones de programas dinámicas, hechas a medida, que están sujetas a determinadas limitaciones. El sistema determina qué limitaciones se refieren a este servicio y construye la implementación de manera

correspondiente. Por consiguiente, la implementación está hecha a medida especialmente para la aplicación correspondiente. El procedimiento puede utilizarse en particular para componer diferentes reglas o limitaciones, como, por ejemplo, regulaciones de exportación sobre funciones de cifrado y descifrado.

En el documento EP 1 507 211 A1 se describe un aparato de comunicación que encapsula de manera segura datos y procesa los mismos como objeto encapsulado por medio de un programa. Por consiguiente, puede conseguirse un acceso limitado a los datos y con ello seguridad para el usuario.

Igualmente, en el documento WO 03/021427 A2 se describe un procedimiento y un sistema que permite controlar el acceso a distintos niveles funcionales de software. Por consiguiente, puede desarrollarse y entregarse una única versión de software cuya función pueden utilizar los clientes para un desarrollo de software adicional.

El objetivo de la presente invención es proporcionar un procedimiento, así como un módulo de seguridad, que impidan un acceso no autorizado al anclaje de veracidad.

Exposición de la invención

Este objetivo se alcanza mediante las reivindicaciones independientes. Perfeccionamientos ventajosos son objeto de las reivindicaciones dependientes.

La invención reivindica un procedimiento para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato, en el que se ejecutan las siguientes etapas de procedimiento:

- recibir una solicitud para proporcionar una función de seguridad de este tipo,
- proporcionar una interfaz para una entidad, denominada anclaje de veracidad, que pone a disposición una función de seguridad de este tipo,
- en el que dicha interfaz determina una información de contexto dependiendo de la aplicación que inicia la solicitud,
- proporcionar la función de seguridad solicitada para la aplicación que inicia la solicitud,
- en el que la información de contexto determinada se incorpora a la provisión de dicha función de seguridad.

Un perfeccionamiento de la invención prevé que la información de contexto se incorpore como parámetro, por ejemplo, como parámetro de seguridad, a la provisión de la función de seguridad.

La función de seguridad puede proporcionarse de forma que se ejecute. La ejecución puede proporcionar un valor de respuesta. Como valor de respuesta puede concebirse una clave (derivada), una firma y valores de función criptográficos adicionales.

Un perfeccionamiento de la invención prevé que la información de contexto se incorpore como valor de función de un solo sentido a la provisión de la función de seguridad.

Un perfeccionamiento de la invención prevé que la información de contexto modifique y/o influya en el valor resultante de la función de seguridad. En este caso, el valor de función de seguridad se modifica de manera correspondiente después de ejecutar la función de seguridad.

Un perfeccionamiento de la invención prevé que la interfaz transmita la información de contexto determinada al anclaje de veracidad.

Un perfeccionamiento de la invención prevé que la información de contexto se transmita en un formato seguro.

Un perfeccionamiento de la invención prevé que el formato seguro se consiga mediante la conversión por medio de una función de un solo sentido o por medio de una firma o por medio de un código de autenticación o por medio de la generación o la derivación de una clave o de cualquier combinación de los mismos.

Un perfeccionamiento de la invención prevé que la información de contexto comprenda la identidad de dicha aplicación.

A este respecto, la información de contexto puede estar caracterizada por lo siguiente:

- El nombre de la aplicación

- La fecha de creación de la aplicación

- El valor de *hash* mediante el archivo ejecutable

- El nombre de usuario que invoca la aplicación

- El grupo de usuarios que invoca la aplicación

- El ID de proceso del proceso que invoca la aplicación

- El *name space* (espacio de nombres) del proceso o del usuario que invoca la aplicación. Dentro de un espacio de nombres puede llamarse inequívocamente a objetos, por ejemplo, mediante nombres de ruta.

- El nombre o espacio de nombres del aparato mediante el que se llama al ESK (*embedded security kernel*, *kernel* de seguridad incrustado) (por ejemplo, en Linux: “/dev/esk”),

- Un identificador (Security-Enhanced Linux) o un identificador específico de sistema operativo del usuario o del proceso o del aparato o del sistema que accede (rol, nombre de usuario, dominio, tipo, contexto)

- Otros datos (específicos de sistema operativo) mediante la aplicación o el estado actual

Un aspecto adicional de la invención prevé un dispositivo para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato, que presenta:

- medios para recibir una solicitud para proporcionar una función de seguridad de este tipo,
- al menos una interfaz para una entidad, denominada anclaje de veracidad, que pone a disposición una función de seguridad de este tipo,
- en el que dicha interfaz está diseñada para determinar una información de contexto dependiendo de la aplicación que inicia la solicitud,
- medios para proporcionar una función de seguridad para la aplicación que inicia la solicitud, en el que estos medios están diseñados para hacer que se incorpore la información de contexto determinada a la provisión de dicha función de seguridad.

Un aspecto adicional de la invención puede ser un programa informático o un producto de programa informático con medios para realizar el procedimiento y las configuraciones mencionadas del mismo, cuando el (producto de) programa informático se ejecuta en un dispositivo de la técnica mencionada anteriormente.

El dispositivo anterior y, dado el caso, el (producto de) programa informático pueden configurarse o perfeccionarse de manera correspondiente de modo análogo al procedimiento y sus configuraciones o perfeccionamientos.

Además, puede estar previsto un dispositivo de provisión para almacena y/o proporcionar el producto de programa informático. El dispositivo de provisión es, por ejemplo, un soporte de datos que almacena y/o proporciona el producto de programa informático. Alternativa y/o adicionalmente, el dispositivo de provisión es, por ejemplo, un servicio de red, un sistema informático, un sistema de servidor, en particular un sistema informático distribuido, un sistema de computación basado en la nube y/o un sistema de computación virtual, que almacena y/o proporciona el producto de programa informático preferiblemente en forma de un flujo de datos.

Por ejemplo, esta provisión se efectúa como descarga en forma de un bloque de datos de programa y/o un bloque de datos de comando, preferiblemente como archivo, en particular como archivo de descarga, o como flujo de datos, en particular como flujo de datos de descarga, del producto de programa informático completo. No obstante, por ejemplo, esta provisión también puede efectuarse como una descarga parcial que se compone de varias partes y que en particular se descarga mediante una red punto a punto o se proporciona como flujo de datos. Un producto de programa informático de este tipo se lee en un sistema, por ejemplo, usando el dispositivo de provisión en forma de soporte de datos y ejecuta los comandos de programa, de modo que el procedimiento según la invención se ejecuta en un ordenador o el aparato de creación se configura de tal manera que el mismo crea el dispositivo según la invención.

La invención y sus formas de realización presentan las siguientes ventajas:

La ventaja de esta invención se basa en la defensa contra ataques en los que una aplicación de atacante no autorizada quiere obtener acceso al anclaje de veracidad.

Cuando una aplicación de atacante se hace en este caso con un sistema, averigua qué ID de identidad, que también puede comprender datos y parámetros de la aplicación original, utiliza una aplicación original y luego quiere ejecutar

en el anclaje de veracidad la misma operación o función de seguridad, proporciona de vuelta al anclaje de veracidad una función de seguridad que se compone del ID de la aplicación original y de las informaciones de contexto específicas de aplicación de atacante, por ejemplo, el número de proceso o nombre, fecha, *hash*, etc. de la aplicación de atacante.

Ventajas, detalles y perfeccionamientos adicionales de la invención se desprenden de la siguiente descripción de ejemplos de realización en relación con los dibujos.

A este respecto muestran:

la figura 1, el modo de proceder descrito al principio, y

la figura 2, el modo de proceder según la invención cuando a la función de seguridad se le añaden informaciones de identidad/contexto con respecto a la aplicación que invoca, por ejemplo, en el controlador del anclaje de veracidad.

La figura 2 muestra un sistema incrustado ES con un dispositivo E para proporcionar una función de seguridad criptográfica. A este respecto, el sistema incrustado ES comprende aplicaciones, por ejemplo, A, AA. El dispositivo E comprende o se comunica con una entidad que pone a disposición la función de seguridad, también denominada anteriormente anclaje de veracidad V. La comunicación del anclaje de veracidad V con el dispositivo E se efectúa por medio de una interfaz que puede estar configurada, por ejemplo, como controlador T. El controlador (por ejemplo, módulo de *kernel* de Linux) del anclaje de veracidad V permite que al menos una información de contexto se incorpore mediante la aplicación que solicita o invoca la función de seguridad, por ejemplo, A, a la operación de seguridad que se ejecuta o se proporciona por el anclaje de veracidad. Una información de contexto, por ejemplo, en forma de una información de identidad o identificación A_ID de la aplicación que invoca A se incluye en la operación de seguridad. En el ejemplo de realización se muestran en la figura 2 dos aplicaciones A y AA que solicitan al anclaje de veracidad una función de seguridad K. A este respecto, una aplicación original A inicia una solicitud de una función de seguridad K. Una interfaz T del dispositivo E determina además como información de contexto, por ejemplo, una información de identificación A_ID de la aplicación A. en una variante, el controlador transmite al anclaje de veracidad los datos y/o los parámetros obtenidos por la aplicación original, por ejemplo, un parámetro de seguridad SP junto con una información de identificación A_ID determinada dependiendo de la aplicación que invoca. En otra variante, la interfaz forma, por ejemplo, con una función de un solo sentido o de *hash* H(A_ID, SP) un parámetro o un valor de función de *hash* que depende de un parámetro SP que puede predefinirse por la aplicación y la información de identificación A_ID de la aplicación, y transmite el mismo al anclaje de veracidad V. El anclaje de veracidad proporciona de vuelta con la operación de seguridad solicitada una función de seguridad, por ejemplo, como función de firma, como función de clave o como función u operación criptográfica adicional. En una variante adicional, el controlador puede modificar el mensaje de respuesta recibido por el anclaje de veracidad, que puede comprender un resultado de la función de seguridad K(SP), dependiendo de la información de identificación determinada de la aplicación A y proporcionar el valor modificado K' (A_ID, SP) de la aplicación A. En el caso de la aplicación de atacante se proporcionaría a la aplicación AA con una invocación idéntica del dispositivo E un valor de respuesta K' (AA_ID, SP) diferente desde el dispositivo. Todos los modos de proceder representados anteriormente también pueden combinarse entre sí.

Posibles informaciones de contexto de este tipo serían entre otras (individualmente o en combinación):

- El nombre de la aplicación

- La fecha de creación de la aplicación

- El valor de *hash* mediante el archivo ejecutable

- El nombre de usuario que invoca la aplicación

- El grupo de usuarios que invoca la aplicación

- La ID de proceso del proceso que invoca la aplicación

- El *name space* (espacio de nombres) del proceso o del usuario que invoca la aplicación. Dentro de un espacio de nombres puede llamarse inequívocamente a objetos, por ejemplo, mediante nombres de ruta.

- El nombre o espacio de nombres del aparato, mediante el que se llama al ESK (*embedded security kernel*, *kernel* de seguridad incrustado) (por ejemplo, en Linux: "/dev/esk"),

- Un identificador (Security-Enhanced Linux) o un identificador específico de sistema operativo del usuario o del proceso o del aparato o del sistema que accede (rol, nombre de usuario, dominio, tipo, contexto)

- Otros datos (específicos de sistema operativo) sobre la aplicación o el estado actual

De manera análoga a la aplicación original A, una aplicación de atacante AA puede acceder al anclaje de veracidad V. Incluso si la aplicación de atacante AA conociera la información de identificación A_ID de la aplicación original A, de este modo se incluye a este respecto una segunda información de identificación AA_ID de la aplicación de atacante AA en la función de seguridad K del anclaje de veracidad V. Por consiguiente, sólo pueden proporcionarse de vuelta a la aplicación de atacante AA resultados de funciones de seguridad en las que está incluida la segunda información de la aplicación de atacante AA. Luego, la aplicación de atacante AA obtiene un valor de respuesta K(AA_ID, SP) o K'(AA_ID, SP) (por ejemplo, una clave derivada) que no coincide con el valor de respuesta K(A_ID, SP) o K'(A_ID, SP) (por ejemplo, clave derivada) de la aplicación original A.

Para atacar satisfactoriamente un sistema de este tipo la aplicación de atacante AA tendría que atacar partes del sistema operativo. Eso es apenas posible o dado el caso sólo es posible con un esfuerzo muy grande. Además, no es necesario limitar a un anclaje de veracidad el acceso a un dispositivo o una interfaz, lo que no puede ponerse en práctica técnicamente con frecuencia y estaría relacionado con un alto esfuerzo de configuración. A este respecto se permite que una aplicación de atacante u otra aplicación acceda al anclaje de veracidad. No obstante, se consigue que la aplicación de atacante u otra aplicación no pueda invocar la misma función de seguridad que la primera aplicación.

Aunque la invención en detalle se ilustró y describió más detalladamente mediante el ejemplo de realización preferido, de este modo la invención no está limitada por los ejemplos dados a conocer y el experto en la técnica puede derivar otras variaciones sin apartarse del alcance de protección de la invención.

REIVINDICACIONES

1. Procedimiento para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato, en el que se ejecutan las siguientes etapas de procedimiento:

   - recibir una solicitud para proporcionar una función de seguridad (K) de este tipo,
   - proporcionar una interfaz (T) para una entidad, denominada anclaje de veracidad (V), que pone a disposición una función de seguridad de este tipo,
   - en el que dicha interfaz determina una información de contexto (A_ID, AA_ID) dependiendo de la aplicación (A, AA) que inicia la solicitud,
   - proporcionar la función de seguridad solicitada para la aplicación que inicia la solicitud,
   - en el que la información de contexto determinada se incorpora a la provisión de dicha función de seguridad, caracterizado porque

   la información de contexto comprende la identidad de dicha aplicación.

2. Procedimiento según la reivindicación anterior, caracterizado porque la información de contexto se incorpora como parámetro a la provisión de la función de seguridad.

3. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la información de contexto se incorpora como valor de función de un solo sentido a la provisión de la función de seguridad.

4. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la información de contexto modifica y/o influye en el valor (K') resultante de la función de seguridad.

5. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la interfaz transmite la información de contexto determinada al anclaje de veracidad.

6. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la información de contexto se transmite en un formato seguro.

7. Procedimiento según la reivindicación anterior, caracterizado porque el formato seguro se consigue mediante la conversión por medio de una función de un solo sentido o por medio de una firma o por medio de un código de autenticación o por medio de la generación o la derivación de una clave.

8. Dispositivo (E) para proporcionar una función de seguridad criptográfica para el funcionamiento de un aparato, que presenta:

   - medios para recibir una solicitud para proporcionar una función de seguridad (K) de este tipo,
   - al menos una interfaz (T) para una entidad, denominada anclaje de veracidad (V), que pone a disposición una función de seguridad de este tipo,
   - en el que dicha interfaz está diseñada para determinar una información de contexto (A_ID, AA_ID) dependiendo la aplicación (A, AA) que inicia la solicitud,
   - medios para proporcionar una función de seguridad (K) para la aplicación que inicia la solicitud, en el que estos medios están diseñados para hacer que se incorpore la información de contexto determinada a la provisión de dicha función de seguridad, caracterizado porque

   la información de contexto comprende la identidad de dicha aplicación.

9. Dispositivo según la reivindicación anterior, caracterizado porque la información de contexto se incorpora como parámetro a la provisión de la función de seguridad.

10. Dispositivo según una de las reivindicaciones de dispositivo anteriores, caracterizado porque la información de contexto se incorpora como valor de función de un solo sentido a la provisión de la función de seguridad.

11. Dispositivo según una de las reivindicaciones de dispositivo anteriores, caracterizado porque la información de contexto está diseñada para modificar y/o influir en el valor (K') resultante de la función de seguridad.

12. Dispositivo según una de las reivindicaciones de dispositivo anteriores, caracterizado porque la interfaz está

diseñada para transmitir la información de contexto determinada al anclaje de veracidad.

13. Dispositivo según una de las reivindicaciones de dispositivo anteriores, caracterizado porque la información de contexto puede transmitirse en un formato seguro.

14. Dispositivo según la reivindicación anterior, caracterizado porque el formato seguro puede conseguirse mediante conversión por medio de una función de un solo sentido o por medio de una firma o por medio de un código de autenticación o por medio de la generación o la derivación de una clave.

15. Programa informático con medios para realizar el procedimiento según una de las reivindicaciones de procedimiento anteriores, cuando el programa informático se ejecuta en un dispositivo (E) según una de las reivindicaciones de dispositivo anteriores.

FIG 1 Estado de la técnica

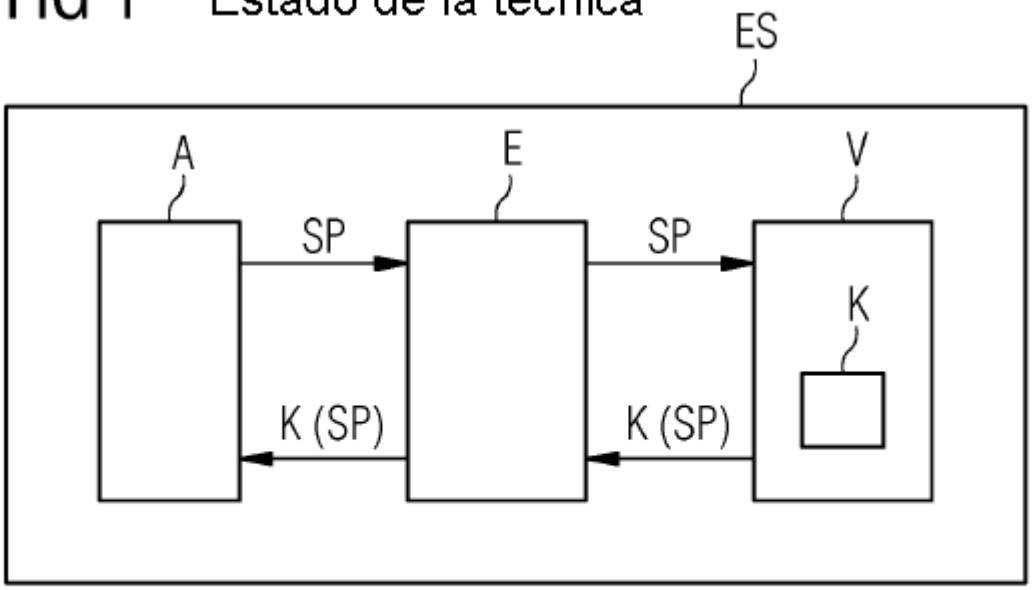

FIG 2