(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 651 177**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.05.2015 E 15169536 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.09.2017 EP 2963579**

(54) Título: **Procedimiento de gestión de la instalación de una aplicación en un dispositivo electrónico**

(30) Prioridad:

04.07.2014 FR 1456498

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.01.2018

(73) Titular/es:

SCHNEIDER ELECTRIC INDUSTRIES SAS (100.0%)
35 rue Joseph Monier
92500 Rueil-Malmaison, FR

(72) Inventor/es:

MOULIN, MICHEL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de gestión de la instalación de una aplicación en un dispositivo electrónico

La presente invención se refiere a un procedimiento de gestión de la instalación de una aplicación de software en un dispositivo electrónico. La invención se refiere igualmente a un procedimiento de generación de un paquete de software y al producto de programa informático asociado. La invención se refiere igualmente a un dispositivo electrónico.

Los dispositivos electrónicos han recurrido cada vez más frecuentemente a unas aplicaciones integradas. Un autómata programable o un disyuntor son dos ejemplos de dichos dispositivos electrónicos.

Las aplicaciones integradas tienen necesidad periódicamente de una actualización, particularmente cuando aparecen mejoras de la aplicación o se corrigen defectos. Durante la instalación de una nueva versión de la aplicación en un dispositivo electrónico, es importante verificar que la nueva versión es adecuada para el dispositivo electrónico considerado y que la nueva versión ha sido generada por una empresa habilitada (un suministrador acordado o el fabricante del dispositivo electrónico). En efecto, La instalación de una versión modificada por un tercero malicioso es susceptible de impedir el funcionamiento del dispositivo, aún peor, implicar un funcionamiento del dispositivo peligroso para el usuario.

Es deseable por tanto actualizar las aplicaciones de un dispositivo electrónico autenticando con seguridad la procedencia de cualquier actualización.

Para ello, es conocida la utilización de firmas electrónicas presentes en la actualización de la aplicación, estando provisto el dispositivo electrónico de medios de identificación de firmas electrónicas específicas. A modo de ejemplo, el documento EP-A-2.402.879 describe una herramienta de aplicación que permite generar una firma adecuada de la aplicación que comprende un generador de código para la producción de un código binario, un generador de certificados separados de los códigos binarios y una plataforma que asocia al menos un certificado a al menos un código binario para facilitar la actualización de las aplicaciones integradas en un dispositivo electrónico.

El documento US 2007/055881 A1 describe un procedimiento que permite sustituir un certificado por un nuevo certificado a continuación de la verificación de las firmas relacionadas con dicho nuevo certificado. Los documentos EP 2.744.244 A1 (párrafo 69) y US 2007/214453 (párrafo 162) divulgan una autenticación de la aplicación basada en la utilización de una pluralidad de certificados. Con el fin de que autenticación tenga éxito, es suficiente que al menos una de las firmas asociadas corresponda a la firma de la aplicación. No obstante, al buscar la industria minimizar las pérdidas de explotación, los dispositivos electrónicos se actualizan poco frecuentemente, por ejemplo durante varios años de funcionamiento. De hecho, cuando el dispositivo electrónico no se ha actualizado desde hace mucho tiempo y se han creado en el intervalo varias versiones de la firma de la aplicación, los medios de identificación del dispositivo electrónico son capaces de identificar solamente unas firmas electrónicas que han pasado a estar obsoletas. El documento antes mencionado no permite gestionar eficazmente una situación de ese tipo.

Existe por tanto una necesidad de un procedimiento de gestión de la instalación de una aplicación de software en un dispositivo electrónico que garantice una instalación segura, comprendiendo en ella el caso en el que los medios de identificación del dispositivo electrónico sean capaces de identificar solamente unas firmas electrónicas que han pasado a estar obsoletas.

A tal efecto, se propone un procedimiento de gestión de la instalación de una aplicación de software en un dispositivo electrónico. El dispositivo electrónico incluye una memoria en la que se memoriza una clave pública de autenticación de la aplicación y una clave pública de autenticación del certificado. El paquete de software incluye una aplicación de software que comprende al menos un código ejecutable. El paquete de software incluye también una primera firma de autenticación de la aplicación obtenida mediante una codificación asimétrica que utiliza una primera clave privada de encriptado. El paquete de software incluye igualmente un certificado que comprende unas informaciones. El paquete de software comprende también una segunda firma de autenticación del certificado, siendo la segunda firma un conjunto de al menos una segunda sub-firma de autenticación del certificado, siendo obtenida cada segunda sub-firma mediante una codificación asimétrica cada una utilizando una segunda clave privada de encriptado respectiva, siendo distinta al menos una de las segundas claves privadas de encriptado de la primera clave privada de encriptado. El procedimiento comprende una etapa de investigación de la autenticidad de la segunda firma con ayuda de la clave pública de autenticación del certificado, siendo autenticado el certificado si al menos una de las segundas sub-firmas se considera como auténtica durante la realización de la etapa de investigación.

El procedimiento de gestión de la instalación de una aplicación de software en un dispositivo electrónico garantiza por tanto una instalación de seguridad, comprendiendo en ella el caso en el que los medios de identificación del dispositivo electrónico sean capaces de identificar solamente unas firmas electrónicas que han pasado a estar obsoletas.

Según unos modos de realización particulares, el procedimiento de instalación comprende una o varias de las características siguientes, tomada(s) aisladamente o según cualquier combinación técnicamente posible:

- al menos una de las segundas claves privadas de encriptado se asocia a la clave pública de autenticación del certificado.
- la etapa de investigación se realiza únicamente cuando la primera firma se considera como no auténtica utilizando la clave pública de autenticación de la aplicación.
- el procedimiento incluye además la etapa de renovación de la clave pública de autenticación de la aplicación del dispositivo electrónico y de la clave pública de autenticación del certificado del dispositivo electrónico.
- las informaciones del certificado incluyen una primera clave pública asociada a la primera clave privada de encriptado y la aplicación incluye una segunda clave pública asociada a una segunda clave privada de encriptado, siendo la primera clave pública la nueva clave pública de autenticación de la aplicación obtenida como resultado de la etapa de renovación y siendo la segunda clave pública la nueva clave pública de autenticación del certificado obtenida como resultado de la etapa de renovación.
- el procedimiento incluye, además, una etapa de autenticación de la aplicación por verificación de la autenticidad de la primera firma con ayuda de la nueva clave pública de autenticación de la aplicación.
- la instalación de la aplicación es rechazada cuando al menos uno de entre el certificado y la aplicación se considera como no auténtico.

Se propone igualmente un procedimiento de generación de un paquete de software que comprende una etapa de suministro de una aplicación que comprende al menos un ejecutable, una primera clave privada de encriptado, un certificado que comprende unas informaciones y al menos una segunda clave privada de encriptado, siendo distinta al menos una de las segundas claves privadas de encriptado de la primera clave privada de encriptado. El procedimiento de generación incluye también una etapa de generación de una primera firma de autenticación de la aplicación con ayuda de una codificación asimétrica que utiliza la primera clave privada de encriptado, y una etapa de generación de una segunda firma de autenticación del certificado, siendo la segunda firma un conjunto de al menos una segunda sub-firma de autenticación del certificado, comprendiendo la etapa de generación de la segunda firma la obtención de cada segunda sub-firma mediante la utilización de un encriptado asimétrico con ayuda de una segunda clave privada de encriptado respectiva.

Se propone igualmente un producto programa informático que incluye unas instrucciones de software que, cuando las instrucciones de software se ejecutan por un ordenador realizan un procedimiento de generación tal como se ha descrito anteriormente.

Se propone también un dispositivo electrónico que incluye una memoria en la que se memoriza una clave pública de autenticación del certificado y una clave pública de autenticación de la aplicación, Siendo distintas la clave pública de autenticación del certificado y la clave pública de autenticación de la aplicación.

Surgirán otras ventajas y características de la invención con la lectura de la descripción que sigue de modos de implementación de la invención, dada a título de ejemplo únicamente y con referencia los dibujos que son:

- figura 1, una representación esquemática de un ejemplo de disyuntor que comprende una pluralidad de dispositivos electrónicos,
- figura 2, una representación esquemática de un ejemplo de un paquete de software según un primer modo de realización,
- figura 3, un organigrama de un ejemplo de implementación de un procedimiento de generación que permite generar el paquete de software de la figura 2,
- figura 4, un organigrama de un ejemplo de implementación de un procedimiento de instalación según un primer modo de realización,
- figura 5, una representación esquemática de un ejemplo de paquete de software según un segundo modo de realización,
- figura 6, un organigrama de un ejemplo de implementación de un procedimiento de generación que permite generar el paquete de software de la figura 5, y
- figura 7, un organigrama de un ejemplo de implementación de un procedimiento de instalación según un primer modo de realización.

Por convención, en lo que sigue de la descripción, se entiende un módulo en el sentido amplio, y es sinónimo de medio.

En la figura 1, un disyuntor eléctrico 8 comprende una unidad de disparo, no representada, y un sistema electrónico 10. La unidad de disparo es conocida por sí misma, y no se describe más en detalle.

El sistema electrónico 10 comprende cuatro dispositivos electrónicos 12A, 12B, 12C, 12D, a saber un primer dispositivo 12A, un segundo dispositivo 12B, un tercer dispositivo 12C y un cuarto 12D, y un bus de comunicación 13 que conecta entre sí los dispositivos electrónicos 12A, 12B, 12C, 12D.

Los dispositivos electrónicos 12A, 12B, 12C, 12D son, por ejemplo, un dispositivo de interfaz hombre-máquina. Igualmente designado por FDM (en inglés *Front Display Module),* un dispositivo de interfaz de red, por ejemplo un dispositivo de interfaz con una red Modbus, igualmente designado por IFM (en inglés *Interface Modbus),* un dispositivo de interfaz con la unidad de disparo del disyuntor 8, tal como un dispositivo designado por BCM (en inglés

Breaker Control Module) o también un dispositivo designado por BSCM (en inglés *Breaker Status Control Module).* Los dispositivos electrónicos 12A, 12B, 12C, 12D son igualmente, por ejemplo, un dispositivo de mantenimiento, igualmente designado por UTA (en inglés *USB Tool Adaptator)* o BU (en inglés *Base unit)* y un dispositivo de entradas/salidas, igualmente designado Módulo E/S (en inglés *Input/Output Module*).

El primer dispositivo electrónico 12A es, según el ejemplo de la figura 1, el dispositivo de mantenimiento UTA mientras que el segundo dispositivo electrónico 12B es un dispositivo de interfaz hombre-máquina FDM, el tercer dispositivo electrónico 12C es un dispositivo de interfaz de red IFM y el cuarto dispositivo electrónico 12D es un dispositivo de interfaz BCM con la unidad de disparo del disyuntor eléctrico 8.

El primer dispositivo electrónico 12A incluye un primer módulo 14A de comunicación con uno o varios dispositivos electrónicos 12B, 12C, 12D del conjunto. El primer dispositivo electrónico 12A incluye igualmente una primera unidad de procesamiento de informaciones 16A formada por ejemplo por una primera memoria 18A y un primer procesador 20A asociado a la primera memoria 18A.

El segundo dispositivo electrónico 12B, respectivamente el tercer dispositivo electrónico 12C y respectivamente el cuarto dispositivo electrónico 12D incluyen los mismos elementos que el primer dispositivo electrónico 12A descrito anteriormente, reemplazando cada vez primero por segundo, respectivamente por tercero y respectivamente por cuarto, elementos para los que la referencia se obtiene sustituyendo la letra A por la letra B, respectivamente por la letra C y respectivamente por la letra D. En la figura 1, los elementos contenidos en el cuarto dispositivo electrónico 12D no se han representado por razones de simplificación de los dibujos.

Cada dispositivo electrónico 12A, 12B, 12C, 12D incluye una o varias funciones materiales y/o de software no representadas.

Se entiende por función material, cualquier función realizada por un componente material (en inglés *hardware*), es decir por un componente electrónico o por un conjunto de componentes electrónicos. Cada componente electrónico es, por ejemplo, una memoria electrónica adaptada para memorizar unos datos, un componente de entradas/salidas, un componente de interfaz con un enlace de comunicación, tal como un enlace serie, un enlace USB, un enlace Ethernet, un enlace Wi-Fi u otros. A modo de ejemplo suplementario, un componente electrónico es un componente lógico programable, igualmente denominado FPGA (en inglés *Field Programmable Gate Array)*, o también un circuito integrado dedicado, igualmente denominado ASIC (en inglés *Application Specific Integrated Circuit)* o cualquier otro componente electrónico, programable o no.

Se entiende por función de software, cualquier función realizada por un componente de software, tanto si se trata de un programa de base (en inglés *firmware*) o incluso un programa de aplicación (en inglés *software*). Una función del software se entiende así en el sentido amplio como un conjunto de instrucciones de programación adecuadas para realizar dicha función de software cuando se ejecutan las instrucciones de software por un procesador.

En lo que sigue, el primer dispositivo electrónico 12A se considera más específicamente, sabiendo que la invención propuesta se aplica igualmente a los otros dispositivos electrónicos 12B, 12C, 12D.

El bus de comunicación 13 es, por ejemplo, un bus por cable, interno del disyuntor 8 y que une los dispositivos electrónicos 12A, 12B, 12C, 12D. El bus 13 está adaptado para permitir un intercambio de datos entre los dispositivos electrónicos 12A, 12B, 12C, 12D. Los módulos de comunicación 14A, 14B, 14C, 14D son entonces unos módulos de interface con el bus de comunicación 13.

Como variante, no representada, el bus de comunicación 13 tiene la forma de un enlace radioeléctrico de datos, y los módulos de comunicación 14A, 14B, 14C, 14D son entonces unos módulos radioeléctricos de comunicación.

La primera memoria 18A es apropiada para memorizar una clave pública C1 de autenticación de la aplicación y una primera función de cifrado H1.

La primera memoria 18A es igualmente apropiada para memorizar una clave pública C2 de autenticación del certificado y una segunda función de cifrado H2.

La clave pública C2 de autenticación del certificado y la clave pública C1 de autenticación de la aplicación son distintas.

Preferentemente, la segunda función de cifrado H2 es distinta de la primera función de cifrado H1. Esto permite aumentar la seguridad durante la instalación de una aplicación.

El primer procesador 20A es, para el caso del primer dispositivo electrónico 12A, apropiado para ejecutar una inicialización (en inglés *boot*). En el caso en el que el primer dispositivo electrónico 12A soporta múltiples aplicaciones, una inicialización es capaz de aislar la aplicación a instalar de las otras aplicaciones instaladas. Esto permite proteger al primer dispositivo electrónico 12A si una aplicación a instalar en el primer dispositivo electrónico 12A resulta ser una aplicación maliciosa.

La inicialización ejecutada por el primer procesador 20A es apropiada para autenticar una aplicación utilizando la

clave pública C1 de autenticación de la aplicación.

La inicialización ejecutada por el primer procesador 20A es igualmente apropiada para autenticar un certificado utilizando la clave pública C2 de autenticación del certificado.

La inicialización ejecutada por el primer procesador 20A es también apropiada para proceder a la instalación de una aplicación de software. La inicialización ejecutada por el primer procesador 20A es así apropiada para gestionar la instalación de una aplicación que forma parte de un paquete de software 100 tal como se ha representado esquemáticamente en la figura 2.

El paquete de software 100 incluye una aplicación 102, un certificado 104, una primera firma FWSC (en inglés *Firmware Signature Code)* de autenticación de la aplicación 102 y una segunda firma CSC (en inglés *Certificate Signature Code)* de autenticación del certificado 104.

Según otra variante, el paquete de software 100 comprende una pluralidad de aplicaciones 102 y una primera firma relativa a ciertas aplicaciones específicas 102. No obstante, como este caso se reduce al caso de un módulo de extensión, no se describe ya en lo que sigue.

Según el ejemplo de la figura 2, la aplicación 102 es un software de base.

Como variante, la aplicación 102 es un módulo de extensión (en inglés *add-on* o *plugin).*

La aplicación 102 incluye un conjunto de datos. En el caso ilustrado por la figura 2, los datos de la aplicación 102 son un archivo de ejecución 110. El archivo de ejecución 110 incluye el conjunto de los códigos ejecutables que aseguran el funcionamiento de la aplicación 102.

En el caso de la figura 2, el conjunto de los datos de la aplicación 102 no están encriptados. Como variante, el conjunto de los datos de la aplicación 102 están encriptados.

El certificado 104 incluye igualmente un conjunto de datos. En el caso ilustrado por la figura 2, los datos del certificado 104 son los datos 112 relativos al suministrador del paquete de software 100 y una primera clave pública FSPK. La primera clave pública FSPK permite desencriptar la primera firma FWSC.

En el caso de la figura 2, el conjunto de los datos del certificado 104 no están encriptados. Como variante, el conjunto de los datos del certificado 104 están encriptados.

La primera firma FWSC y la segunda firma CSC se generan de manera similar (codificación asimétrica) pero a partir de claves privadas distintas. Para ilustrar más específicamente una característica de ese tipo, se hace referencia a la figura 3 que muestra el organigrama de un ejemplo de implementación de un ejemplo de procedimiento de generación del paquete de software 100.

El procedimiento de generación incluye una etapa 200 de suministro de la aplicación 102 y del certificado 104.

El procedimiento de generación incluye una primera etapa 202 de generación. En la primera etapa 202 de generación, se genera la primera firma FWSC de autenticación de la aplicación 102.

La primera etapa 202 de generación incluye una primera subetapa 204 de suministro, una primera subetapa 206 de cálculo y una primera subetapa 208 de encriptado.

En la primera subetapa 204 de suministro, se suministra una primera clave privada SFK (del inglés *Secret Firmware Key).*

En la primera subetapa 206 de cálculo, la primera función de cifrado H1 se aplica a la aplicación 102 para obtener un primer valor de cálculo P1.

En la primera subetapa 208 de encriptado, el primer valor de cálculo P1 obtenido como resultado de la primera subetapa 206 de cálculo se encripta con la ayuda de la primera clave privada SFK proporcionada por una infraestructura de gestión de claves.

El conjunto de las primeras subetapas 206 de cálculo y 208 de encriptado permite realizar una codificación asimétrica utilizando la primera clave privada SFK.

De este modo, la primera firma FWSC se obtiene mediante una codificación asimétrica utilizando la primera clave privada SFK. Como se ha explicado anteriormente, la primera firma FWSC puede desencriptarse utilizando la primera clave pública FSPK, asociándose la primera clave pública FSPK a la primera clave privada SFK.

El procedimiento de generación incluye una segunda etapa 210 de generación. En la segunda etapa 210 de generación, se genera la segunda firma CSC de autenticación del certificado 104.

Preferentemente, como es el caso en el ejemplo de la figura 3, para disminuir el tiempo de implementación del

procedimiento de generación, las dos etapas 202 y 210 de generación se implementan simultáneamente.

La segunda etapa 210 de degeneración incluye una segunda subetapa 212 de suministro, una segunda subetapa 214 de cálculo y una segunda subetapa 216 de encriptado.

En la segunda subetapa 212 de suministro, se proporciona una segunda clave privada SCK (del inglés *Secret Certificate Key).*

En la segunda subetapa 214 de cálculo, se aplica la segunda función de cifrado H2 al certificado 104 para obtener un segundo valor de cálculo P2.

En la segunda subetapa 216 de encriptado, el segundo valor de cálculo P2 obtenido como resultado de la segunda subetapa 214 de cálculo se encripta con la ayuda de la segunda clave privada SCK suministrada.

El conjunto de las segundas subetapas 214 de cálculo y 216 de encriptado permite realizar una codificación asimétrica utilizando la segunda clave privada SCK.

De este modo, la segunda firma CSC se obtiene mediante una codificación asimétrica utilizando la segunda clave privada SCK. Una segunda clave pública FMPK asociada a la segunda clave privada SCK permite desencriptar la segunda firma CSC.

El funcionamiento del primer dispositivo electrónico 12A en el caso de la instalación de la aplicación 102 se describe con referencia a la figura 4 que ilustra un ejemplo de implementación del procedimiento de gestión de la instalación de la aplicación 102 en el primer dispositivo electrónico 12A.

Se entiende por instalación tanto la adición de una aplicación no presente en el primer dispositivo electrónico 12A como la modificación de una versión antigua de la aplicación de software mediante una actualización.

El procedimiento de gestión incluye una primera etapa 300 de prueba de la primera firma FWSC con ayuda de la clave pública C1 de autenticación de la aplicación.

Para autenticar la primera firma FWSC, el primer procesador 20A del primer dispositivo electrónico 12A extrae la primera función de cifrado H1 de la primera memoria 18A, posteriormente aplica la primera función de cifrado H1 a la aplicación 102. El primer procesador 20A obtiene así un primer valor V1.

El primer procesador 20A del primer dispositivo electrónico 12A extrae igualmente la clave pública C1 de autenticación de la aplicación memorizada en la primera memoria 18A. Posteriormente, el primer procesador 20A desencripta la primera firma FWSC con ayuda de la clave pública C1 de autenticación de la aplicación. El primer procesador 20A obtiene así un segundo valor V2.

Es posible demostrar que la primera firma FWSC y la aplicación 102 son auténticas únicamente en el caso en el que el primer valor V1 y el segundo valor V2 son iguales.

El primer procesador 20A del primer dispositivo electrónico 12A compara por tanto el primer valor V1 y el segundo valor V2. Si los dos valores V1, V2 son iguales, el primer procesador 20A del primer dispositivo electrónico 12A autentica la primera firma FWSC mientras que si los dos valores V1, V2 son diferentes, el primer procesador 20A del primer dispositivo electrónico 12A no autentica la primera firma.

En el caso en el que la primera firma FWSC es autenticada, se asegura la procedencia de la aplicación 102 y el procedimiento de gestión incluye a continuación una etapa 350 de instalación de la aplicación 102.

En caso contrario, esto muestra que la clave pública C1 de autenticación de la aplicación FSPK no permite autenticar la nueva aplicación 102.

El procedimiento de gestión incluye entonces una etapa 302 de investigación de la autenticidad de la segunda firma CSC con ayuda de la clave pública C2 de autenticación del certificado.

La implementación de la etapa 302 de investigación por el primer procesador 20A es similar a la implementación de la etapa 300 de prueba y por lo tanto no se describe más específicamente en lo que sigue.

En el caso en el que la segunda firma CSC no se considere como auténtica durante la implementación de la etapa 302 de investigación, el certificado 104 no se autentica. Esto significa que el certificado 104 no proviene de una fuente segura.

De hecho, el procedimiento incluye una etapa 340 de rechazo de la instalación de la aplicación 102 para proteger al primer dispositivo electrónico 12A.

Por el contrario, cuando la segunda firma CSC se considera como auténtica, se autentica el certificado 104. Esto muestra que la clave pública C1 de autenticación de la aplicación no permite ya autenticar la nueva aplicación 102 y más específicamente la primera firma FWSC.

El procedimiento de gestión incluye entonces una etapa 304 de renovación de la clave pública C1 de autenticación de la aplicación del primer dispositivo electrónico 10A.

La etapa 304 de renovación incluye una subetapa 306 de extracción y una subetapa 308 de memorización.

En la subetapa 306 de extracción, la primera clave pública FSPK contenida en los datos del certificado 104 es leída y posteriormente extraída. La subetapa 306 de extracción se implementa por el primer procesador 20A.

Durante la subetapa 308 de memorización, la primera clave pública FSPK reemplaza la antigua clave pública C1 de autenticación de la aplicación.

El procedimiento de gestión incluye también una segunda etapa 310 de prueba de la autenticidad de la primera firma FWSC con la ayuda de la nueva clave pública FSPK de autenticación de la aplicación.

En el caso en el que la primera firma FWSC no se considera como auténtica durante la implementación de la segunda etapa 310 de prueba, la aplicación 102 no se autentica. Esto significa que la aplicación 102 no proviene de una fuente segura. De hecho, la etapa 340 de rechazo de la instalación de la aplicación 102 para proteger al primer dispositivo electrónico 12A es, a continuación, implementada.

Por el contrario, a partir de que se considere como auténtica la primera firma FWSC, se autentica la aplicación 102. Se implementa entonces la etapa 350 de instalación de la aplicación 102.

El procedimiento de gestión permite entonces asegurar que el conjunto del paquete de software 100 se ha generado correctamente por una empresa habilitada (un suministrador acordado o el fabricante del primer dispositivo electrónico 12A).

El procedimiento de gestión permite igualmente garantizar que el paquete de software 100 no se ha modificado por un tercero.

El procedimiento de gestión permite igualmente la renovación de la clave pública de autenticación de la aplicación del primer dispositivo electrónico 10A.

En un modo de realización de ese tipo, la segunda clave privada SCK continúa siendo la misma a todo lo largo de la duración de la vida del primer dispositivo electrónico 12A. Una condición de ese tipo es poco práctica cuando el fabricante del primer dispositivo electrónico 12A es distinto al suministrador del paquete de software 100.

Para ello, se propone igualmente un segundo modo de realización que permite un cambio para la segunda clave privada SCK.

El segundo modo de realización del procedimiento de gestión se describe con referencia a las figuras 1, 5, 6 y 7.

El primer dispositivo electrónico 12A es idéntico en los dos modos de realización.

Los elementos similares entre el paquete de software 100 según el primer modo de realización y el paquete de software 100 según el segundo modo de realización ilustrado por la figura 5 no se repiten en lo que sigue. Solo se ponen en evidencia las diferencias.

En el caso de la figura 5, los datos de la aplicación 102 comprenden, además del archivo de ejecución 110, la segunda clave pública FSPK.

Además, la segunda firma CSC del certificado 104 no es ya una firma única sino un conjunto de segundas sub-firmas indicadas genéricamente por CSCi, haciendo i referencia a un número entero superior a 1. La segunda clave pública FSPK es, en un caso de ese tipo, una clave que permite descifrar una de las segundas sub-firmas CSCi.

La generación de la segunda firma CSC se detalla con referencia a la figura 6 mostrando un organigrama de un ejemplo de la implementación de un ejemplo de procedimiento de generación del paquete de software 100 según el segundo modo de realización. Solo se describe más específicamente la segunda etapa 210 de generación, las otras etapas permanecen sin cambiar con relación al procedimiento de generación descrito con referencia a la figura 3.

En la segunda etapa 210 de generación, se genera la segunda firma CSC de autenticación del certificado 104.

La segunda etapa 210 de generación incluye una subetapa 220 de suministro de un conjunto de claves privadas de encriptado SCKi, haciendo i referencia a un número entero superior a 1.

Las claves de encriptado SCKi suministradas corresponden al conjunto de las claves privadas SCKi que han existido para el primer dispositivo electrónico 12A. Esto significa que al menos una de las segundas claves privadas de encriptado SCKi se asocia a la clave pública C2 de autenticación del certificado 104. En lo que sigue, se supone que es la segunda clave de encriptado indicada por SCK2 la que se asocia a la clave pública C2 de autenticación del certificado 104.

La segunda etapa 210 de generación incluye a continuación la subetapa 214 de cálculo durante la que se aplica la segunda función de cifrado H2 al certificado 104 para obtener el segundo valor de cálculo P2.

La segunda etapa 210 de generación incluye entonces, para cada segunda sub-firma CSCi, una subetapa 222i de encriptado del segundo valor de cálculo P2 con la ayuda de la segunda clave privada SCKi respectiva suministrada para obtener la segunda sub-firma CSCi.

Cada subetapa 222i se implementa, preferentemente, en paralelo. Esto se representa esquemáticamente en la figura 6 mediante la mención a las etapas 2221, 2222 y 222i.

De este modo, la segunda firma CSC se obtiene mediante una codificación asimétrica que utiliza el conjunto de las segundas claves privadas SCKi. La segunda clave pública FMPK asociada a una de las segundas claves privadas SCK, como la clave pública C2 de autenticación del certificado 104 permite desencriptar al menos una de las segundas sub-firmas CSCi.

Preferentemente, las segundas sub-firmas CSCi se ordenan según un orden predefinido, generalmente desde el más reciente al más antiguo pero pueden plantearse otros órdenes.

Según un caso particular, la segunda clave pública FMPK se asocia a la segunda clave privada SCKi más reciente.

Según otro caso particular que corresponde al caso de un dispositivo electrónico 12A antiguo, la segunda clave pública FMPK se asocia a la segunda clave privada SCKi más antigua.

Además, según un modo de realización preferido, cada segunda clave privada de encriptado SCKi es distinta de la primera clave privada de encriptado SFK para garantizar una seguridad óptima.

El procedimiento de gestión se modifica igualmente en el segundo modo de realización tal como lo muestra la figura 7.

La etapa 302 de investigación de la autenticidad de la segunda firma CSC con la ayuda de la clave pública C2 de autenticación del certificado es diferente en el caso del segundo modo de realización.

En efecto, en el caso general, se prueban sucesivamente una pluralidad de segundas sub-firmas CSCi hasta que al menos se autentique una segunda sub-firma CSCi.

En este caso, por ejemplo, la segunda sub-firma CSC1 se descarta porque se considera como no auténtica. La segunda sub-firma CSC2 se prueba y valida a continuación.

La segunda firma CSC no se valida si no puede validarse ninguna de las segundas sub-firmas CSCi.

Además, según el segundo modo de realización, el procedimiento de gestión incluye entonces una etapa 320 de renovación de la clave pública C2 de autenticación del certificado 104 del primer dispositivo electrónico 12A.

La etapa 320 de renovación incluye una subetapa 326 de extracción y una subetapa 328 de memorización.

En la subetapa 326 de extracción, la segunda clave pública FMPK contenida en los datos de la aplicación 102 es leída y posteriormente extraída. La subetapa 326 de extracción se implementa por el primer procesador 20A.

Durante la subetapa 328 de memorización, la segunda clave pública FMPK reemplaza a la antigua clave pública C2 de autenticación del certificado 104.

Una memorización de ese tipo permite autenticar los futuros certificados.

El procedimiento de gestión según el segundo modo de realización presenta las mismas ventajas que el procedimiento de gestión según el primer modo de realización. Además, el procedimiento de gestión según el segundo modo de realización permite una utilización más flexible de las claves privadas, pudiendo variar las claves privadas en el transcurso del ciclo de vida del primer dispositivo electrónico 12A.

Además, el procedimiento de gestión se aplica a cualquier tipo de dispositivo electrónico susceptible de ser actualizado por la instalación de una aplicación de software. De este modo, aunque el procedimiento de gestión se ha ilustrado para una aplicación en el primer dispositivo electrónico 12A, el procedimiento de gestión se aplica igualmente a los otros dispositivos electrónicos 12B, 12C y 12D.

De manera adicional, el primer dispositivo electrónico 12A puede formar parte de otros sistemas distintos a un disyuntor. En concreto, el primer dispositivo electrónico 12A puede formar parte de un autómata programable, de un variador de velocidad, de un ondulador o de una alimentación ininterrumpida de tipo UPS.

REIVINDICACIONES

1. Procedimiento de gestión de la instalación de una aplicación de software (102) en un dispositivo electrónico (12A, 12B, 12C, 12D) que incluye una memoria (18A, 18B, 18C, 18D) en el que se memoriza una clave pública de autenticación de la aplicación (C1) y una clave pública de autenticación del certificado (C2), formando parte la instalación de software de un paquete de software (100) que incluye:

- la aplicación (102) que comprende al menos un ejecutable,
- una primera firma (FWSC) de autenticación de la aplicación (102), habiendo sido obtenida la primera firma (FWSC) mediante una codificación asimétrica que utiliza una primera clave privada (SFK) de encriptado,
- un certificado (104) que comprende unas informaciones, y
- una segunda firma (CSC) de autenticación del certificado (104), siendo la segunda firma un conjunto que comprende unas segundas sub-firmas (CSC, CSCi) de autenticación del certificado, siendo obtenida cada segunda sub-firma (CSC, CSCi) mediante una codificación asimétrica cada una utilizando una segunda clave privada de encriptado respectiva (SCK, SCKi), siendo distinta al menos una de las segundas claves privadas de encriptado (SCK, SCKi) de la primera clave privada (SFK) de encriptado,

el procedimiento comprende la prueba de la primera firma (FWSC) de autenticación de la aplicación (102) con la ayuda de la clave pública de autenticación de la aplicación (C1) y:

- la instalación de la aplicación (102), cuando la primera firma (FWSC) se considera como auténtica, o
- cuando la primera firma (FWSC) de autenticación de la aplicación se considera como no auténtica, el procedimiento comprende además al menos:

  ○ investigación de la autenticidad de la segunda firma (CSC) de autenticación del certificado con la ayuda de la clave pública de autenticación del certificado (C2), siendo autenticado el certificado (104) si al menos una de las segundas sub-firmas (CSC, CSCi) se considera como auténtica durante la implementación de la etapa de investigación, ○ la renovación de la clave pública de autenticación de la aplicación (C1) cuando la segunda firma (CSC) de autenticación del certificado se considera como auténtica,
  ○ la instalación de la aplicación (102), cuando con la ayuda de la nueva clave pública de autenticación de la aplicación, la primera firma (FWSC) de autenticación de la aplicación (102) se considera como auténtica

2. Procedimiento de gestión según la reivindicación 1, en el que al menos una de las segundas claves privadas (SCK, SCKi) de encriptado se asocia a la clave pública de autenticación del certificado (C2).

3. Procedimiento de gestión según una cualquiera de las reivindicaciones 1 a 2, en el que el procedimiento incluye, además, una etapa de renovación de la clave pública de autenticación del certificado (C2) del dispositivo electrónico (12A, 12B, 12C, 12D).

4. Procedimiento de gestión según la reivindicación 3, en el que las informaciones del certificado (104) incluyen una primera clave pública (FSPK) asociada a la primera clave privada de encriptado (SFK) y la aplicación (102) incluye una segunda clave pública (FMPK) asociada a una segunda clave privada de encriptado (SCK), siendo la segunda clave pública de autenticación de la aplicación obtenida como resultado de la etapa de renovación de la primera clave pública (FSPK) y siendo la nueva clave pública de autenticación del certificado obtenida como resultado de la etapa de renovación de la segunda clave pública (FMPK).

5. Procedimiento de gestión según la reivindicación 4, en el que el procedimiento incluye además una etapa de autenticación de la aplicación (102) por verificación de la autenticidad de la primera firma (FWSC) con la ayuda de la nueva clave pública de autenticación de la aplicación.

6. Procedimiento de gestión según la reivindicación 4 o 5, en el que el dispositivo electrónico (12A, 12B, 12C, 12D) incluye un procesador (20A, 20B, 20C) apropiado para ejecutar una inicialización, siendo implementado el procedimiento de gestión por la inicialización.

7. Procedimiento de gestión según una cualquiera de las reivindicaciones 1 a 6, en el que la instalación de la aplicación (102) se rechaza cuando al menos uno del certificado y de la aplicación (102) se considera como no auténtico.

8. Procedimiento de generación de un paquete de software (100) que comprende las etapas de:

- suministro de una aplicación (102) que comprende al menos un ejecutable (110), de una primera clave privada (SFK) de encriptado, de un certificado (104) que comprende unas informaciones y al menos una segunda clave privada de encriptado (SCKi), siendo distinta al menos una de las segundas claves privadas de encriptado (SCK, SCKi) de la primera clave privada (SFK) de encriptado,
- generación de una primera firma (FWSC) de autenticación de la aplicación (102) con la ayuda de una codificación asimétrica que utiliza la primera clave privada (SFK) de encriptado, y
- generación de una segunda firma (CSC) de autenticación del certificado (104), siendo la segunda firma un conjunto que comprende unas segundas sub-firmas (CSC, CSCi) de autenticación del certificado,

comprendiendo la etapa de generación de la segunda firma (CSC) la obtención de cada segunda sub-firma (CSC, CSCi) mediante la utilización de una codificación asimétrica con la ayuda de una segunda clave privada de encriptado respectiva (SCK, SCKi).

9. Producto de programa informático que incluye unas instrucciones de software que, cuando las instrucciones de software se ejecutan por un ordenador implementan un procedimiento de generación según la reivindicación 8.

10. Dispositivo electrónico (12A, 12B, 12C, 12D) que incluye una memoria (18A, 18B, 18C, 18D) en la que se memoriza una clave pública de autenticación del certificado (C2) y una clave pública de autenticación de la aplicación (C1), siendo distintas la clave pública de autenticación del certificado (C2) y la clave pública de autenticación de la aplicación (C1) y un procesador (20A, 20B, 20C) configurado para implementar las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 8.

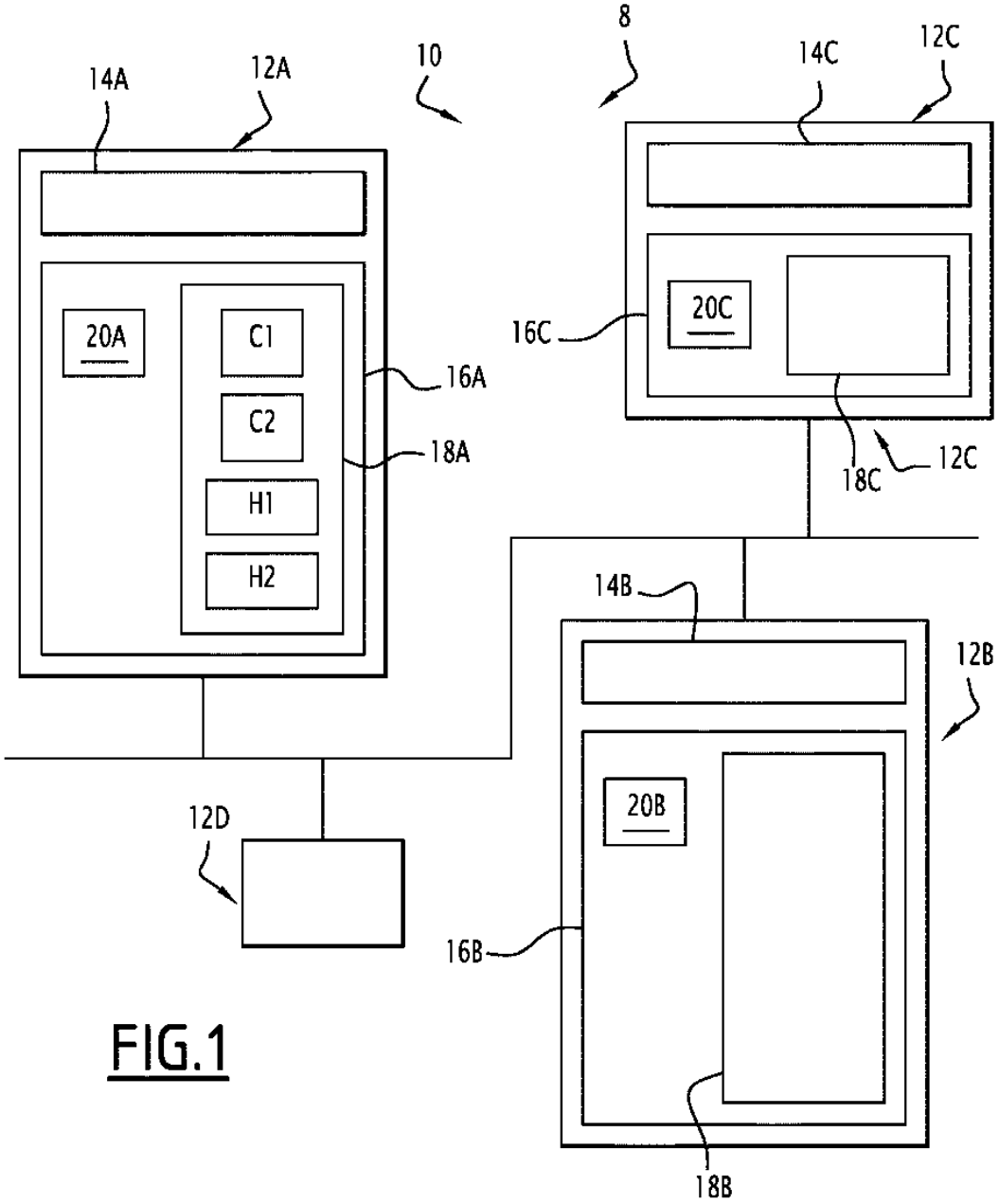
14A
12A
10
8
14C
12C
20A
C1
C2
H1
H2
16A
18A
16C
20C
18C
12C
14B
12B
12D
20B
16B
18B

FIG.1

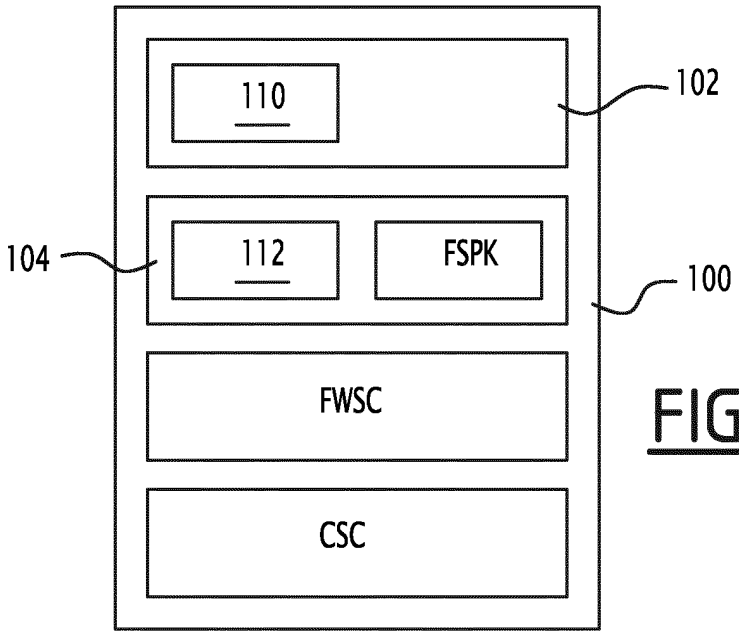
110
102
104
112
FSPK
100
FWSC
CSC

FIG.2

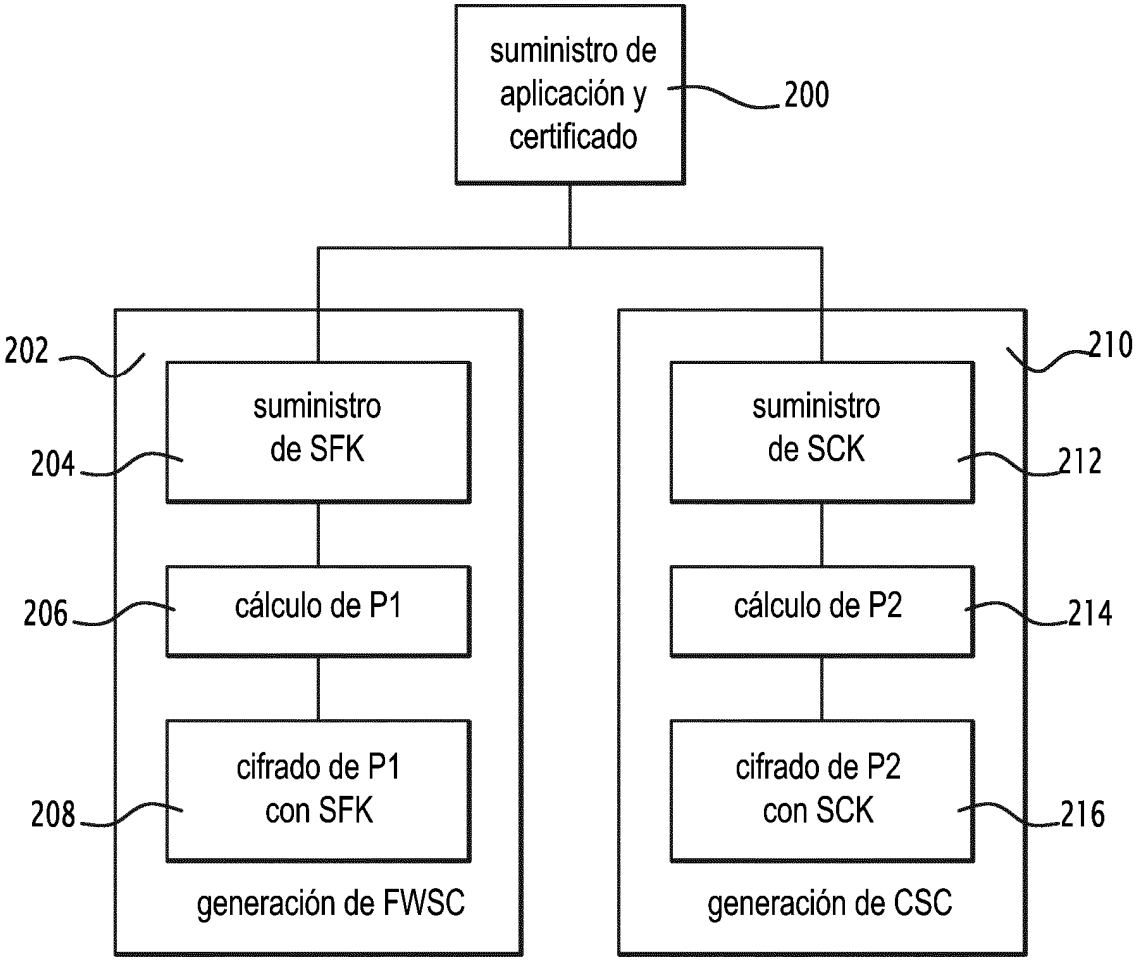
suministro de aplicación y certificado
200
202
210
suministro de SFK
204
suministro de SCK
212
cálculo de P1
206
cálculo de P2
214
cifrado de P1 con SFK
208
cifrado de P2 con SCK
216
generación de FWSC
generación de CSC

FIG.3

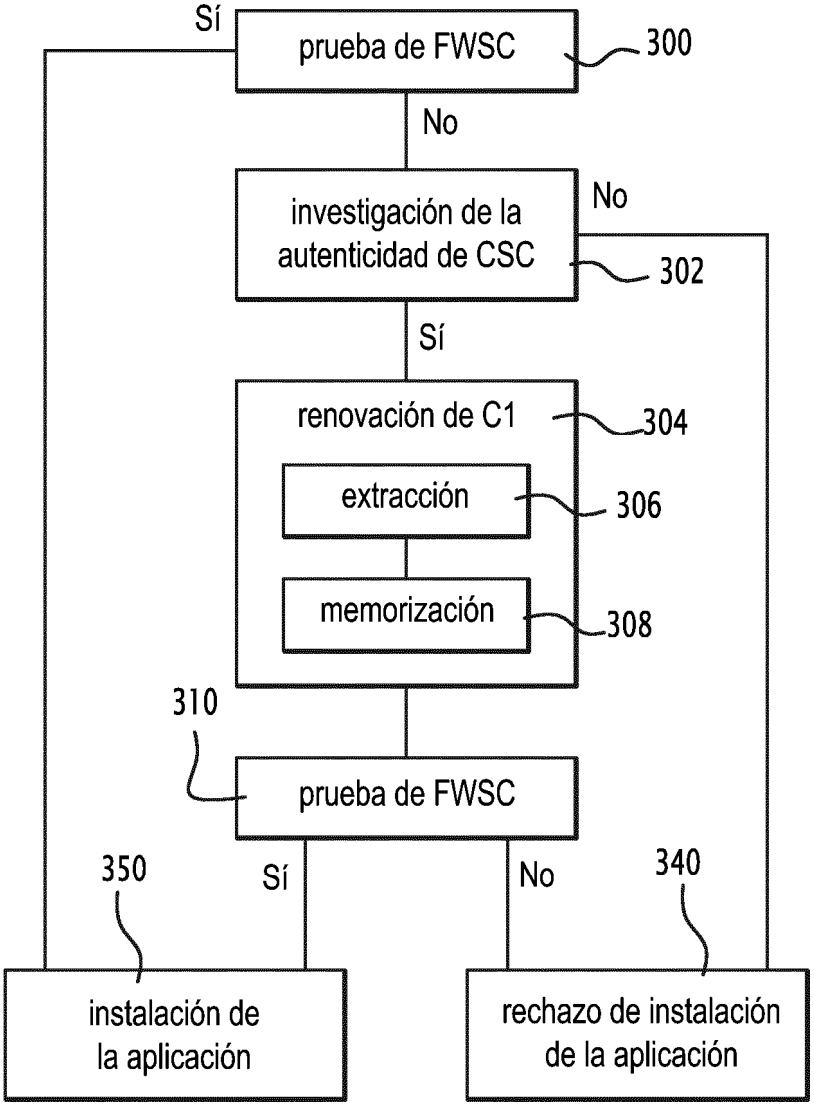
Sí
prueba de FWSC
300
No
investigación de la autenticidad de CSC
No
302
Sí
renovación de C1
304
extracción
306
memorización
308
310
prueba de FWSC
350
Sí
No
340
instalación de la aplicación
rechazo de instalación de la aplicación

FIG.4

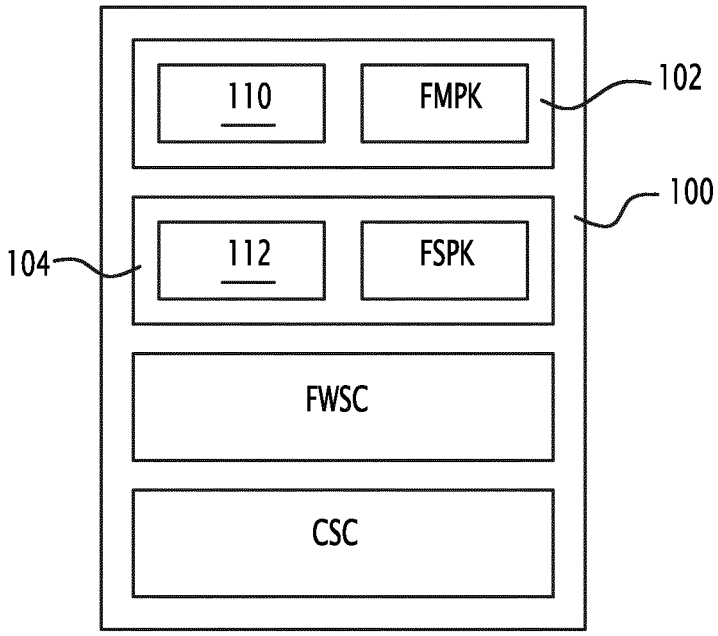

FIG.5

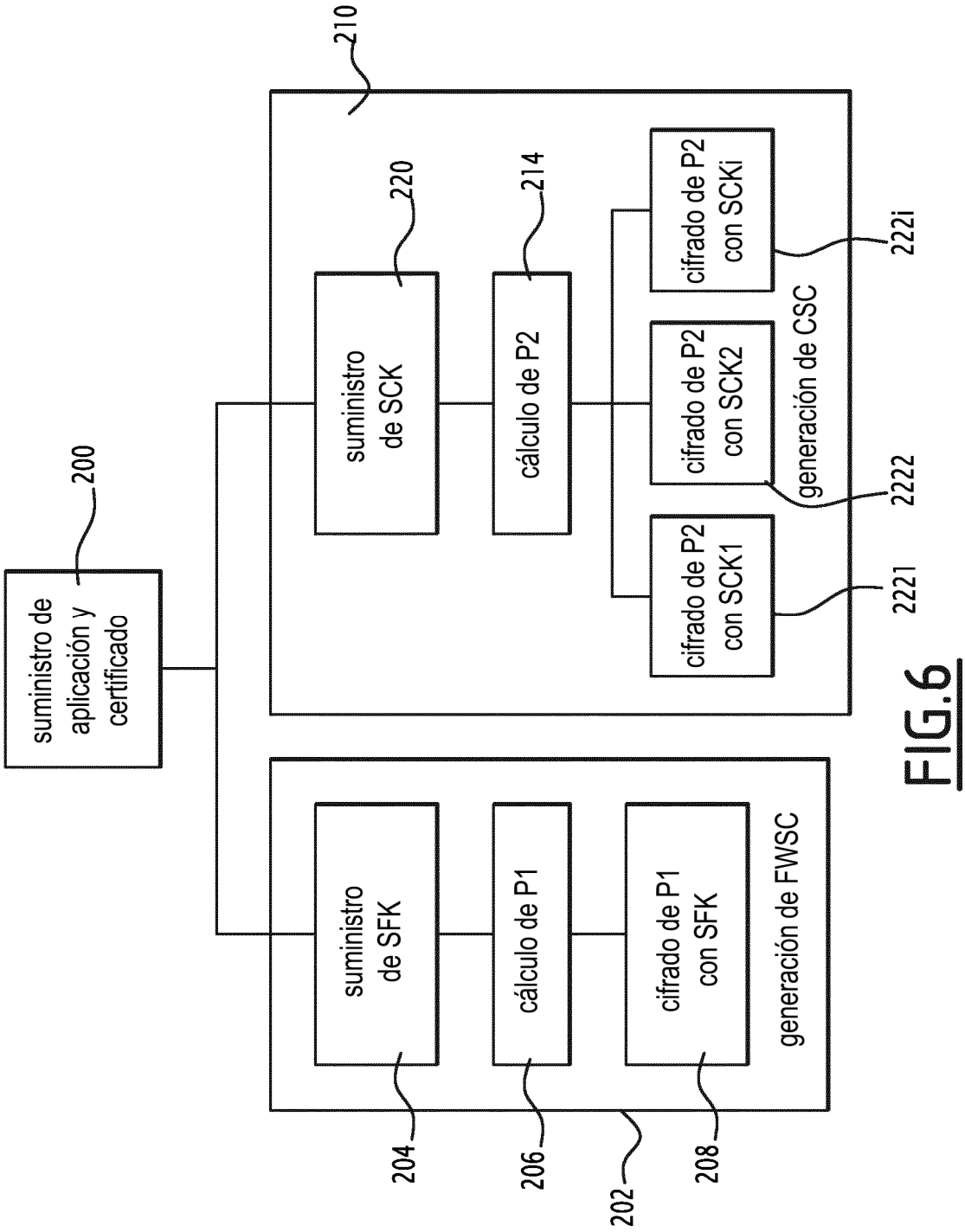
suministro de aplicación y certificado
200
210
suministro de SCK
220
cálculo de P2
214
cifrado de P2 con SCK1
cifrado de P2 con SCK2
cifrado de P2 con SCKi
generación de CSC
2221
2222
222i
suministro de SFK
cálculo de P1
cifrado de P1 con SFK
generación de FWSC
204
206
202
208

FIG.6

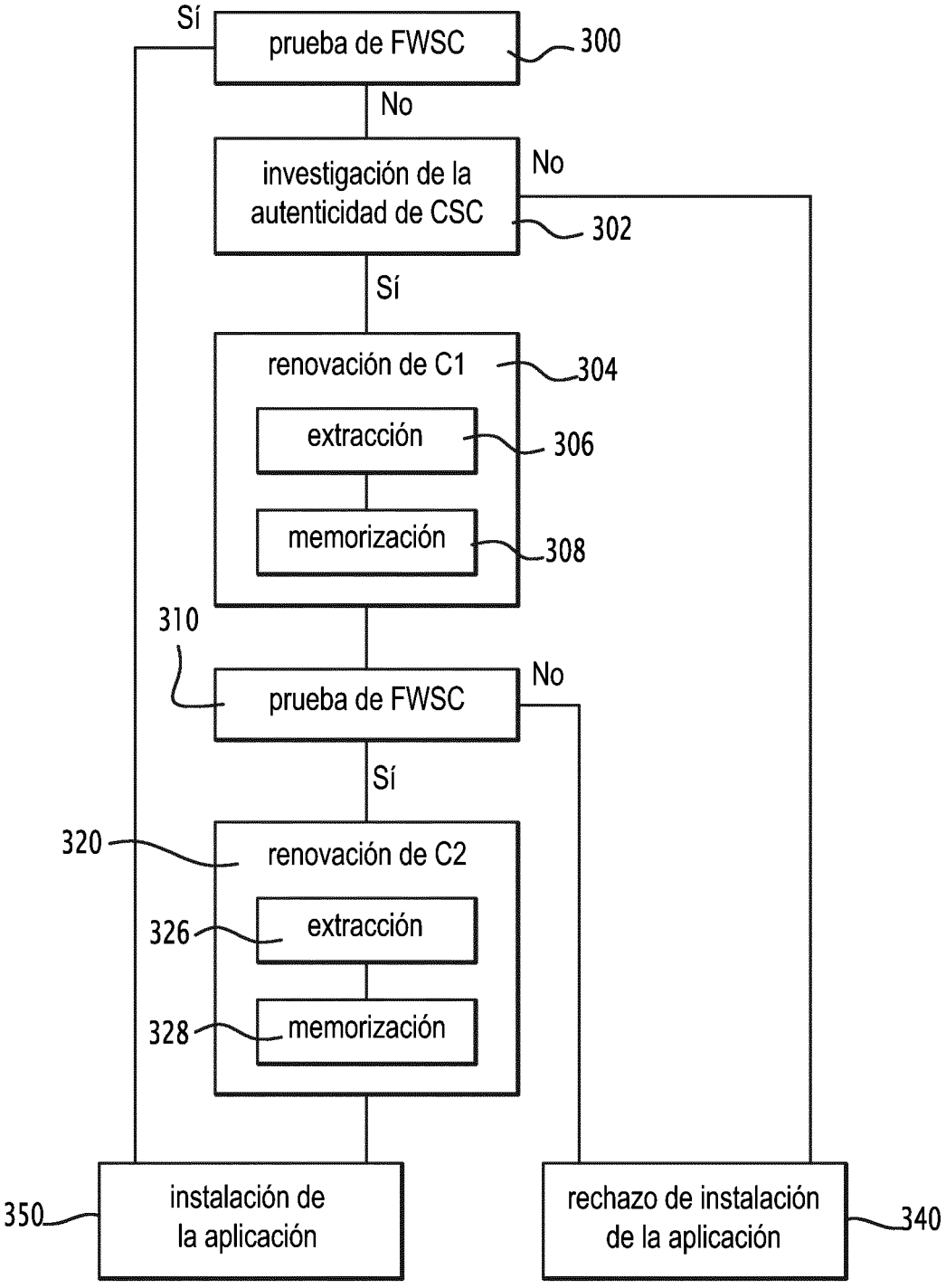
Sí
prueba de FWSC
300
No
investigación de la autenticidad de CSC
No
302
Sí
renovación de C1
304
extracción
306
memorización
308
310
prueba de FWSC
No
Sí
320
renovación de C2
326
extracción
328
memorización
instalación de la aplicación
350
rechazo de instalación de la aplicación
340

FIG.7