(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 660 837**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.09.2013 PCT/EP2013/069090**

(87) Fecha y número de publicación internacional: **22.05.2014 WO14075830**

(96) Fecha de presentación y número de la solicitud europea: **16.09.2013 E 13766921 (4)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2018 EP 2891266**

(54) Título: **Procedimiento y configuración para una comunicación segura entre equipos de red en una red de comunicación**

(30) Prioridad:

16.11.2012 DE 102012220990

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.03.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

PYKA, STEFAN y
ZWANZGER, JOHANNES

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y CONFIGURACIÓN PARA UNA COMUNICACIÓN SEGURA ENTRE EQUIPOS DE RED EN UNA RED DE COMUNICACIÓN

DESCRIPCIÓN

La presente invención se refiere a un procedimiento y una configuración para la comunicación segura entre equipos de red en una red de comunicación.

A menudo se desea proteger frente a ataques exteriores un software a ejecutar en un equipo de red inseguro, como por ejemplo una plataforma de hardware insegura. Una plataforma de hardware insegura, como por ejemplo un ordenador universal compuesto por componentes estándar, no presenta ninguna contramedida frente a tales ataques desde el exterior sobre un software que corre en la plataforma. Los ataques exteriores tienen por ejemplo como finalidad obtener informaciones sobre el software que corre o bien manipular el software.

Para implementar en una plataforma de hardware insegura medidas que cumplan determinadas exigencias de seguridad para el software que corre, existen distintos enfoques.

Si la correspondiente plataforma de hardware no puede ampliarse o modificarse, deben lograrse todas las medidas para asegurar el software mediante una ampliación del software existente. Son medios conocidos por ejemplo la técnica de la ofuscación o la llamada criptografía White-Box (de caja blanca), que permiten ocultar frente a un atacante la forma de funcionamiento así como los contenidos en datos de un software que corre en la plataforma de hardware. Desde luego estas técnicas implican el peligro de que pese a ello la forma de funcionamiento pueda ser analizada y quebrantada por un atacante.

Si la plataforma de hardware debe ampliarse o modificarse, se ofrece la posibilidad de utilizar equipos de red seguros adecuados, como por ejemplo módulos seguros. Son módulos seguros por ejemplo módulos Secure-Memory (de memoria segura), módulos Trusted-Plattform (TPMs, de plataforma de confianza) o controladores Smart Card (de tarjeta inteligente). Mediante tales módulos es posible por ejemplo almacenar material de datos secreto de manera segura y no legible e implementar algoritmos criptográficos con seguridad, por ejemplo de manera resistente a ataques de canal lateral.

La utilización de módulos de hardware seguros implica no obstante el inconveniente de que debido a la comunicación adicionalmente necesaria entre la plataforma insegura y los módulos de hardware seguros pueden surgir otros problemas. Por ejemplo podría interceptar un atacante la interfaz de comunicación entre la plataforma insegura y un módulo seguro y analizar el correspondiente tráfico de datos. Una comunicación confidencial y auténtica entre una plataforma de hardware insegura y un módulo seguro es por lo tanto difícil de garantizar hasta ahora.

La solicitud de patente norteamericana US2007/121947 da a conocer procedimientos y equipos para proporcionar un sistema de gestión de claves para redes de comunicación inalámbricas.

Por ello es un objetivo de la presente invención lograr una comunicación segura mejorada entre equipos de red.

En consecuencia se propone un procedimiento para la comunicación segura entre un primer equipo de red y un segundo equipo de red en una red de comunicación. El primer equipo de red incluye al menos un componente de hardware seguro para el almacenamiento seguro y ejecución segura de un software. El segundo equipo de red incluye al menos un componente de software seguro para la memorización segura y la ejecución segura de un software. El procedimiento presenta las siguientes etapas:

a) almacenamiento de un primer secreto común, de un primer algoritmo y de un segundo algoritmo en el primer equipo de red utilizando el componente de hardware seguro y en el segundo equipo de red utilizando el componente de software seguro;
b) envío de un primer dato desde el segundo equipo de red al primer equipo de red;
c) ejecución del primer algoritmo en el primer equipo de red utilizando el componente de hardware seguro y en el segundo equipo de red utilizando el componente de software seguro para aportar correspondientemente un segundo secreto común, formándose la entrada para el primer algoritmo en cada caso mediante el primer secreto común y el primer dato;
d) envío de un segundo dato desde el primer equipo de red al segundo equipo de red;
e) ejecución del segundo algoritmo en el primer equipo de red utilizando el componente de hardware seguro y en el segundo equipo de red utilizando el componente de software seguro para aportar correspondientemente un tercer secreto común, formándose la entrada para el segundo algoritmo en cada caso mediante el segundo secreto común y el segundo dato y
f) utilización del tercer secreto común mediante el primer equipo de red y el segundo equipo de red para una comunicación segura entre el primer equipo de red y el segundo equipo de red.

El concepto software incluye aquí programas ejecutables y los correspondientes datos y forma el complemento al concepto hardware, que incluye los componentes físicos de un equipo de red.

El primer y el segundo dato pueden enviarse en respectivos textos explícitos, es decir, sin encriptación.

El procedimiento permite una comunicación segura y auténtica entre dos equipos de red, como por ejemplo una plataforma de hardware insegura y un módulo seguro. Entonces es posible configurar diferentes los secretos comunes utilizados para cada par de primer y segundo equipos de red, para que un potencial atacante no pueda transmitir los resultados de un análisis relativo a un equipo de red inseguro a otro equipo de red inseguro.

El procedimiento posibilita proteger de manera flexible el canal de comunicación entre una plataforma insegura y un Security Controller frente a ataques a la confidencialidad y a la autenticidad. Esto se realiza con una complejidad mínima y un coste mínimo.

En formas de realización del procedimiento se ejecuta, para una actualización del tercer secreto común, según una regla que puede prescribirse, una repetición de las etapas d) y e).

De esta manera puede modificarse el tercer secreto común por ejemplo a intervalos regulares, para dificultar un ataque potencial a un canal de comunicación entre el primer y el segundo equipo de red.

El segundo dato se cambia entonces ventajosamente para cada repetición de las etapas d) y e).

En otras formas de realización del procedimiento rechaza el primer equipo de red continuar la comunicación con el segundo equipo de red cuando no existe la actualización que caduca del tercer secreto común, según la regla que puede prescribirse.

Esto significa una mejora adicional de la comunicación segura entre los equipos de red, ya que en el caso de un ataque con éxito no puede seguir utilizando un atacante un tercer secreto común posiblemente corrompido debido a la actualización forzosamente necesaria para continuar la comunicación.

En otras formas de realización incluye la regla que puede prescribirse un activador (trigger), activándose el trigger al transcurrir un intervalo de tiempo que puede prescribirse.

En otras formas de realización incluye la regla que puede determinarse un trigger, activándose el trigger al alcanzarse un volumen de datos intercambiado que puede prescribirse entre el primer equipo de red y el segundo equipo de red.

En otras formas de realización incluye la regla que puede prescribirse un trigger, activándose el trigger tras cada utilización del tercer secreto común por parte del primer equipo de red o del segundo equipo de red.

La actualización del tercer secreto común tras cada utilización es ventajosa por ejemplo cuando se trata de datos a transmitir semánticamente muy sencillos, que sólo pueden asumir pocos valores diferentes, por ejemplo "0/1" o "sí/no". Tales datos puede deducirlos fácilmente un atacante cuando a lo largo de mucho tiempo se utiliza el mismo tercer secreto común para la comunicación segura.

Cuando se cambia regularmente el tercer secreto común, puede analizar un atacante la comunicación sólo durante un breve espacio de tiempo y en todo caso utilizar los resultados hasta que se cambia el tercer secreto común.

En otras formas de realización el primer dato y/o el segundo dato son un número aleatorio, un dato individual de una plataforma o un número de serie.

La utilización de un dato individual de plataforma o de un número de serie posibilita una comunicación individual para una plataforma, que dificulta a un atacante potencial obtener del análisis de la comunicación de una plataforma conclusiones relativas a otras plataformas.

En otras formas de realización se forman el primer secreto común y/o el segundo secreto común y/o el tercer secreto mediante dos claves de comunicación, incluyendo las segundas claves de comunicación una clave de confidencialidad y una clave de autenticidad.

En otras formas de realización el segundo equipo de red es un ordenador universal.

Un ordenador universal es por ejemplo un ordenador o computadora formado por componentes estándar, que no tienen que estar necesariamente asegurados.

En otras formas de realización se configura el componente de hardware seguro mediante un módulo de seguridad protegido frente a un acceso no autorizado.

Un módulo de seguridad es por ejemplo un módulo Trusted-Plattform. Tales módulos de seguridad están disponibles en el mercado en grandes cantidades.

En otras formas de realización está configurado el componente de software seguro mediante ofuscación del código, criptografía White-Box y/o medidas para la protección frente a ataques de debugging (depuración).

Una protección frente a ataques de debugging sirve para proteger frente a ataques al software y/o los correspondientes datos durante el tiempo de marcha mediante los llamados debugger. Los debugger son herramientas de software que posibilitan un acceso a programas en curso y sus datos en la memoria de un ordenador.

En otras formas de realización está configurado el primer equipo de red como Security-Controller, llamado también controlador de Smart Card.

En otras formas de realización está configurado el Security-Controller como componente pasivo.

Pasivo significa aquí que el Security-Controller sólo puede reaccionar a demandas de la plataforma insegura y puede enviar el segundo dato para una actualización de la clave.

Además se propone una configuración con un primer equipo de red y un segundo equipo de red en una red de comunicación. El primer equipo de red incluye al menos un componente de hardware seguro, para el almacenamiento seguro y la ejecución segura de un software y el segundo equipo de red incluye al menos un componente de software seguro para el almacenamiento seguro y la ejecución segura de un software. El componente de hardware seguro está preparado para el almacenamiento seguro de un primer secreto común, de un primer algoritmo y de un segundo algoritmo en el primer equipo de red. El componente de software seguro está preparado para el almacenamiento seguro del primer secreto común, del primer algoritmo y del segundo algoritmo en el segundo equipo de red. La configuración presenta además un primer emisor, que está preparado para enviar un primer dato desde el segundo equipo de red al primer equipo de red. El componente de hardware seguro está preparado para ejecutar con seguridad el primer algoritmo en el primer equipo de red. El componente de software seguro está preparado para ejecutar con seguridad el primer algoritmo en el segundo equipo de red. Ambos sirven para la correspondiente aportación de un segundo secreto común, estando formada la entrada para el primer algoritmo en cada caso por el primer secreto común y el primer dato. La configuración presenta además un segundo emisor, que está preparado para enviar un segundo dato desde el primer equipo de red al segundo equipo de red. Además está preparado el componente de hardware seguro para la ejecución segura del segundo algoritmo en el primer equipo de red. El componente de software seguro está preparado para la ejecución segura del segundo algoritmo en el segundo equipo de red. Ambos sirven para la correspondiente aportación de un tercer secreto común, estando formada la entrada para el segundo algoritmo en cada caso por el segundo secreto común y el segundo dato. Además presenta la configuración elementos de comunicación preparados para utilizar el tercer secreto común mediante el primer equipo de red y el segundo equipo de red para una comunicación segura entre el primer equipo de red y el segundo equipo de red.

El medio criptográfico, el primer y el segundo emisor y los medios de comunicación pueden estar implementados en técnica de hardware y/o también en técnica de software. En una implementación en técnica de hardware puede estar configurado el medio correspondiente como equipo o como parte de un equipo, por ejemplo como computadora o como microprocesador. En una implementación técnica de software puede estar configurado el correspondiente medio como producto de programa de computadora, como una función, como una rutina, como parte de un código de programa o como objeto que puede ejecutarse.

Las características, particularidades y ventajas de esta invención antes descritas, así como la forma como se logran las mismas, quedarán más claras y comprensibles en relación con la siguiente descripción de los ejemplos de realización, que se describirán más en detalle en relación con los dibujos.

Al respecto muestran:

figura 1 una vista esquemática de un ejemplo de realización de una configuración con un primer equipo de red y un segundo equipo de red en una red de comunicación y

figura 2 un diagrama secuencial esquemático de un ejemplo de realización de un procedimiento para la comunicación segura entre un primer equipo de red y un segundo equipo de red en una red de comunicación.

En las figuras se han dotado los mismos elementos o elementos que tienen la misma función de las mismas referencias, siempre que no se indique otra cosa.

La figura 1 muestra en una vista esquemática un primer ejemplo de realización de una configuración 1 con un primer equipo de red Sec y un segundo equipo de red P en una red de comunicación. Entre el primer equipo de red Sec y el segundo equipo de red P existe un enlace de comunicación, que en la figura 1 se representa mediante una línea de trazos. Otros componentes de la red de comunicación no se representan la figura 1 para mayor claridad.

El segundo equipo de red P es un ordenador universal formado por componentes estándar, siendo por ello una plataforma no asegurada o insegura, mientras que el primer equipo de red Sec es un Security-Controller, es decir, una plataforma asegurada o segura.

El Security-Controller Sec incluye un componente de hardware seguro HK, para el almacenamiento seguro y la ejecución segura de un software y la plataforma insegura P incluye un componente de software seguro SK, para el almacenamiento seguro y la ejecución segura de un software. Mediante el componente de software seguro SK está protegido el software, es decir, un programa y sus datos, sobre la plataforma insegura suficientemente frente a ataques de Debugging, con lo que no es posible una lectura rápida por parte de un atacante externo de las claves de comunicación GS, PS y KE, KA utilizadas a continuación sobre la plataforma insegura.

El componente de hardware seguro HK está preparado para almacenar con seguridad un primer secreto común GS y para ejecutar con seguridad un primer algoritmo A1 y un segundo algoritmo A2 en el Security-Controller Sec. El componente de software seguro SK está preparado para almacenar con seguridad el primer secreto común GS y para ejecutar con seguridad el primer algoritmo A1 y el segundo algoritmo A2 en la plataforma insegura P.

Tanto el Security-Controller Sec como también la plataforma insegura P, incluyen así los correspondientes medios para almacenar con seguridad el primer secreto común GS y para ejecutar con seguridad el primer algoritmo A1 y el segundo algoritmo A2. Esto sirve para aportar correspondientemente un segundo secreto común PS.

La plataforma insegura P incluye además un primer emisor S1 para enviar un primer dato SD, por ejemplo un número de serie o una dirección de hardware memorizadas en la plataforma insegura P al Security-Controller Sec.

El Security-Controller P incluye un segundo emisor S2 para enviar un segundo dato R, por ejemplo un número aleatorio, a la plataforma insegura P.

Además están preparados el componente de hardware seguro HK y el componente de software seguro SK para ejecutar con seguridad el segundo algoritmo A2. Esto sirve para proporcionar en cada caso un tercer secreto común KE, KA.

Tanto el Security-Controller Sec como también la plataforma insegura P incluyen un medio de comunicación K1, K2 para utilizar el tercer secreto común KE, KA para una comunicación segura entre sí.

La figura 2 muestra un diagrama secuencial esquemático de un ejemplo de realización de un procedimiento para la comunicación segura entre el Security-Controller Sec y la plataforma insegura P.

En una primera etapa 201 se memoriza el primer secreto común GS, el primer algoritmo A1 y el segundo algoritmo A2 en el Security-Controller utilizando el componente de hardware seguro HK y en la plataforma insegura P utilizando el componente de software seguro SK.

Sobre la plataforma insegura P y sobre el Security-Controller Sec se archiva así un secreto común GS, que puede ser por ejemplo una clave criptográfica en forma de dos claves de comunicación KE, KA. Este secreto común GS es el mismo para todas las plataformas. En el Security-Controller Sec no puede leerse este secreto GS, ya que el Security-Controller Sec incluye por ejemplo una memoria segura, que no puede leerse. Sobre la plataforma insegura P está protegido el secreto común GS con medios adecuados, por ejemplo con ayuda de ofuscación de código o mediante criptografía White-Box, es decir, mediante la integración del secreto GS en un algoritmo criptográfico, que está implementado mediante técnicas de White-Box.

En una segunda etapa 202 se envía el número de serie SD desde la plataforma insegura P al Security-Controller Sec.

La segunda etapa 202 se denomina también Pairing (emparejamiento) inicial.

En una tercera etapa 203 se ejecuta el primer algoritmo A1 sobre el Security-Controller Sec utilizando el componente de hardware seguro HK y sobre la plataforma insegura P utilizando el componente de software seguro SK, para proporcionar correspondientemente el segundo secreto común PS, estando formada la entrada para el primer algoritmo A1 en cada caso por el primer secreto común GS y el número de serie SD.

Se deduce por lo tanto con la ayuda del número de serie SD individual de la plataforma, tanto sobre la plataforma insegura P como también sobre el Security-Controller Sec, en cada caso con el mismo algoritmo A1, un secreto PS individual de la plataforma. El dato SD, aquí el número de serie, puede enviarse en texto explícito al Security-Controller Sec. El algoritmo A1 debe estar protegido sobre la plataforma insegura P por ejemplo mediante ofuscación o criptografía White-Box.

El Security-Controller Sec exige a intervalos regulares una actualización de la clave de comunicación KE, KA. Para ello se realiza en una cuarta etapa 204 un envío del número aleatorio R desde el Security-Controller Sec a la plataforma insegura P.

En una quinta etapa 205 se ejecuta el segundo algoritmo A2 en el Security-Controller Sec utilizando el componente de hardware Seguro HK y en la plataforma insegura P utilizando el componente de software Seguro SK, para proporcionar correspondientemente el tercer secreto común KE, KA, estando formada la entrada para el segundo algoritmo A2 en cada caso por el segundo secreto común PS y el segundo dato R.

De esta manera se calculan a partir del número aleatorio R y de la clave PS individual de la plataforma nuevas claves de comunicación KE, KA, que incluyen una clave de confidencialidad KE y una clave de autenticidad KA. El número aleatorio R puede enviarse a su vez en texto explícito a la plataforma insegura P. El algoritmo A2 debe protegerse en la plataforma insegura P a su vez mediante ofuscación de código o criptografía White-Box.

La cuarta etapa 204 y la quinta etapa 205 son una actualización (update) del secreto o actualización de clave correspondiente a la clave de comunicación. La actualización del secreto se ejecuta con preferencia a intervalos regulares, para dificultar un ataque de un atacante externo.

La plataforma insegura P debe estar forzada a ejecutar a intervalos regulares una actualización de la clave. Este proceso no puede ser activado por el Security-Controller Sec, cuando se trata de un módulo puramente pasivo. Se definen por lo tanto reglas que clarifican inequívocamente para ambas partes, es decir, para el Security-Controller Sec y la plataforma insegura P, cuándo ha de realizarse una tal actualización de la clave. Esto puede ser por ejemplo tras alcanzar una determinada cantidad de datos transmitida entre el Security-Controller Sec y la plataforma insegura P o bien una vez transcurrido un espacio de tiempo que puede prescribirse.

Cuando falta una actualización de la clave caducada según una regla, rechaza el Security-Controller Sec cualquier comunicación adicional con la plataforma insegura P.

En la sexta etapa 206 se realiza una utilización del tercer secreto común KE, KA por parte del Security-Controller Sec y la plataforma insegura P para una comunicación segura entre sí. La sexta etapa 206 incluye entonces una cantidad cualquiera de procesos de comunicación entre el Security-Controller Sec y la plataforma insegura P, realizándose a intervalos de tiempo regulares, tal como antes se ha indicado, una actualización de claves según las etapas 204 y 205, para aumentar aún más la seguridad del procedimiento.

La etapa 202 se utiliza para hacer posible una comunicación individual de la plataforma. Esta medida dificulta que un atacante obtenga a partir del análisis de la comunicación de una plataforma conclusiones relativas a otras plataformas.

Las etapas 204 y 205, es decir, la actualización de las claves con regularidad, se utilizan para dificultar a un atacante el análisis de la comunicación. Puesto que la clave de comunicación se cambia con regularidad, sólo puede analizar un atacante la comunicación durante un corto espacio de tiempo y en todo caso utilizar los resultados hasta que se cambia la clave.

La etapa 202 no puede sustituirse por el envío desde el Security-Controller Sec a la plataforma insegura P de un número aleatorio R2. En ese caso le sería posible a un atacante observar en una plataforma este número aleatorio e introducirlo en otras plataformas (inseguras) en el curso del proceso de Pairing. El Security-Controller Sec desde el que se ha enviado el numero aleatorio R2 podría utilizarse entonces como servidor para distintas plataformas inseguras, ya que entonces todas las plataformas conocerían la misma claves PS individuales de la plataforma.

A continuación se representa un ejemplo de la elección de los algoritmos A1 y A2.

El secreto común GS y el secreto común PS se memorizan sobre la plataforma insegura P mediante un cifrado de bloques E simétrico protegido por criptografía White-Box. El cifrado de bloques E simétrico protegido por criptografía White-Box es así el componente de software Seguro SK sobre la plataforma insegura P.

Las distintas etapas para los algoritmos A1 y A2, inclusive el archivo de la clave o memorización de la clave en la plataforma insegura P y el Security-Controller Sec, son como sigue:

1. GS tiene que protegerse de forma adecuada mediante una transformación irreversible T. Por lo tanto GS está archivado en la plataforma insegura P en forma de T(GS).

2. El cifrado de bloques E simétrico invierte la transformación T, por ejemplo mediante implementación White-Box, sobre la clave GS, realizándose a continuación la derivación de clave propiamente dicha y archivándose el resultado a su vez después de una transformación con T:

   La derivación de PS se realiza mediante PS = $E(T^{-1}(GS), SD)$. Sobre la plataforma P insegura se archiva T(PS).

3. Para generar las claves de comunicación KA y KE, genera el Security-Controller Sec dos números aleatorios R1 y R2. Éstos se encriptan de nuevo con ayuda del algoritmo simétrico A2 y los textos cifrados se utilizan como las dos claves de comunicación KE, KA:

   La deducción de KE se realiza mediante KE = $E(T^{-1}(PS), R1)$.
   La deducción de KA se realiza mediante KA = $E(T^{-1}(PS), R2)$.

Un atacante no puede ahora atacar con éxito el secreto común GS, ya que el mismo está protegido en la plataforma insegura P mediante la transformación T y en el Security-Controller Sec mediante la memoria segura.

Un atacante no puede además atacar con éxito el algoritmo A1, ya que éste está protegido mediante los métodos de White-Box en la plataforma insegura P y mediante la memoria segura en el Security-Controller Sec.

Un atacante tampoco puede atacar con éxito el secreto común PS, ya que el mismo está protegido sobre la plataforma insegura P mediante la transformación T y en el Security-Controller Sec mediante la memoria segura.

Tampoco puede atacar con éxito un atacante el algoritmo A2, ya que el mismo está protegido mediante los métodos de White-Box en la plataforma insegura P y mediante la memoria segura en el Security-Controller Sec.

Además tampoco puede un atacante atacar con éxito las claves de comunicación KE y KA, ya que las mismas, tal como antes se ha descrito, tienen una vida muy corta, debido a la actualización regular de las claves y la plataforma insegura P está suficientemente protegida con medidas anti-Debugging, para impedir una extracción rápida de las claves de comunicación KE, KA de la memoria de la plataforma insegura P. En el Security-Controller Sec están protegidas las claves de comunicación KE y KA mediante la memoria segura.

Aún cuando la invención se ha ilustrado y descrito más en detalle mediante el ejemplo de realización preferido, la invención no queda limitada por los ejemplos dados a conocer y el especialista puede deducir de allí otras variaciones. El ámbito de protección de la invención queda definido por las reivindicaciones.

REIVINDICACIONES

1. Procedimiento para la comunicación segura entre un primer equipo de red (Sec) y un segundo equipo de red (P) en una red de comunicación, en el que el primer equipo de red (Sec) incluye al menos un componente de hardware seguro (HK) para el almacenamiento seguro y la ejecución segura de un software y el segundo equipo de red (P) incluye al menos un componente de software seguro (SK), para la memorización segura y la ejecución segura de un software,
con las etapas:

a) almacenamiento de un primer secreto común (GS), de un primer algoritmo (A1) y de un segundo algoritmo (A2) en el primer equipo de red (Sec) utilizando el componente de hardware seguro (HK) y en el segundo equipo de red (P) utilizando el componente de software seguro (SK);
b) envío de un primer dato (SD) desde el segundo equipo de red (P) al primer equipo de red (Sec);
c) ejecución del primer algoritmo (A1) en el primer equipo de red (Sec) utilizando el componente de hardware seguro (HK) y en el segundo equipo de red (P) utilizando el componente de software seguro (SK) para aportar correspondientemente un segundo secreto común (PS), formándose la entrada para el primer algoritmo (A1) en cada caso mediante el primer secreto común (GS) y el primer dato (SD);
d) envío de un segundo dato (R) desde el primer equipo de red (Sec) al segundo equipo de red (P);
e) ejecución del segundo algoritmo (A2) en el primer equipo de red (Sec) utilizando el componente de hardware seguro (HK) y en el segundo equipo de red (P) utilizando el componente de software seguro (SK) para aportar correspondientemente un tercer secreto común (KE, KA), formándose la entrada para el segundo algoritmo (A2) en cada caso mediante el segundo secreto común (PS) y el segundo dato (R) y
f) utilización del tercer secreto común (KE, KA) mediante el primer equipo de red (Sec) y el segundo equipo de red (P) para una comunicación segura entre el primer equipo de red (Sec) y el segundo equipo de red (P).

2. Procedimiento de acuerdo con la reivindicación 1,
caracterizado porque para una actualización del tercer secreto común (KE, KA), según una regla que puede prescribirse, se ejecuta una repetición de las etapas d) y e).

3. Procedimiento de acuerdo con la reivindicación 2,
caracterizado porque el primer equipo de red (Sec) rechaza continuar la comunicación con el segundo equipo de red (P) cuando no existe la actualización que caduca del tercer secreto común (KE, KA), según la regla que puede prescribirse.

4. Procedimiento de acuerdo con la reivindicación 2 ó 3,
caracterizado porque la regla que puede prescribirse incluye un activador (trigger), activándose el trigger al transcurrir un intervalo de tiempo que puede prescribirse.

5. Procedimiento de acuerdo con la reivindicación 2 ó 3,
caracterizado porque la regla que puede determinarse incluye un trigger, activándose el trigger al alcanzarse un volumen de datos intercambiado que puede prescribirse entre el primer equipo de red (Sec) y el segundo equipo de red (P).

6. Procedimiento de acuerdo con la reivindicación 2 ó 3,
caracterizado porque la regla que puede prescribirse incluye un trigger, activándose el trigger tras cada utilización del tercer secreto común (KE, KA) por parte del primer equipo de red (Sec) o del segundo equipo de red (P).

7. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
caracterizado porque el primer dato (SD) y/o el segundo dato (R) son un número aleatorio, un dato individual de una plataforma o un número de serie.

8. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
caracterizado porque el primer secreto común (GS) y/o el segundo secreto común (PS) y/o el tercer secreto (KE, KA) se forman mediante dos claves de comunicación (KE, KA), incluyendo las dos claves de comunicación (KE, KA) una clave de confidencialidad (KE) y una clave de autenticidad (KA).

9. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
caracterizado porque el segundo equipo de red (P) es un ordenador universal.

10. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
caracterizado porque el componente de hardware seguro (HK) se configura mediante un módulo de seguridad protegido frente a un acceso no autorizado.

11. Procedimiento de acuerdo con una de las reivindicaciones precedentes,

caracterizado porque el componente de software seguro (SK) se configura mediante ofuscación del código, criptografía White-Box y/o medidas para la protección frente a ataques de debugging (depuración).

12. Procedimiento de acuerdo con una de las reivindicaciones precedentes,
caracterizado porque el primer equipo de red (Sec) se configura como controlador de Smart Card.

13. Procedimiento de acuerdo con la reivindicación 12,
caracterizado porque el SmartCard-Controller (Sec) se configura como componente pasivo.

14. Configuración (1) con un primer equipo de red (Sec) y un segundo equipo de red (P) en una red de comunicación,
en la que el primer equipo de red (Sec) incluye al menos un componente de hardware seguro (HK), para el almacenamiento seguro y la ejecución segura de un software y en el que el segundo equipo de red (P) incluye al menos un componente de software seguro (SK) para el almacenamiento seguro y la ejecución segura de un software, en la que
    a) el componente de hardware seguro (HK) está preparado para el almacenamiento seguro de un primer secreto común (GS), de un primer algoritmo (A1) y de un segundo algoritmo (A2) en el primer equipo de red (Sec) y el componente de software seguro (SK) está preparado para el almacenamiento seguro del primer secreto común (GS), del primer algoritmo (A1) y del segundo algoritmo (A2) en el segundo equipo de red (P);
    b) un primer emisor (S1) está preparado para enviar un primer dato (SD) desde el segundo equipo de red (P) al primer equipo de red (Sec);
    c) el componente de hardware seguro (HK) está preparado para ejecutar con seguridad el primer algoritmo (A1) en el primer equipo de red (Sec) y el componente de software seguro (SK) está preparado para ejecutar con seguridad el primer algoritmo (A1) en el segundo equipo de red (P), para la correspondiente aportación de un segundo secreto común (PS), estando formada la entrada para el primer algoritmo (A1) en cada caso por el primer secreto común (GS) y el primer dato (SD);
    d) un segundo emisor (S2) está preparado para enviar un segundo dato (R) desde el primer equipo de red (Sec) al segundo equipo de red (P);
    e) el componente de hardware seguro (HK) está preparado para la ejecución segura del segundo algoritmo (A2) en el primer equipo de red (Sec) y el componente de software seguro (SK) está preparado para la ejecución segura del segundo algoritmo (A2) en el segundo equipo de red (P), para la correspondiente aportación de un tercer secreto común (KE, KA), estando formada la entrada para el segundo algoritmo (A2) en cada caso por el segundo secreto común (PS) y el segundo dato (R) y
    f) elementos de comunicación (K1, K2) preparados para utilizar el tercer secreto común (KE, KA) mediante el primer equipo de red (Sec) y el segundo equipo de red (P) para una comunicación segura entre el primer equipo de red (Sec) y el segundo equipo de red (P).

FIG 1

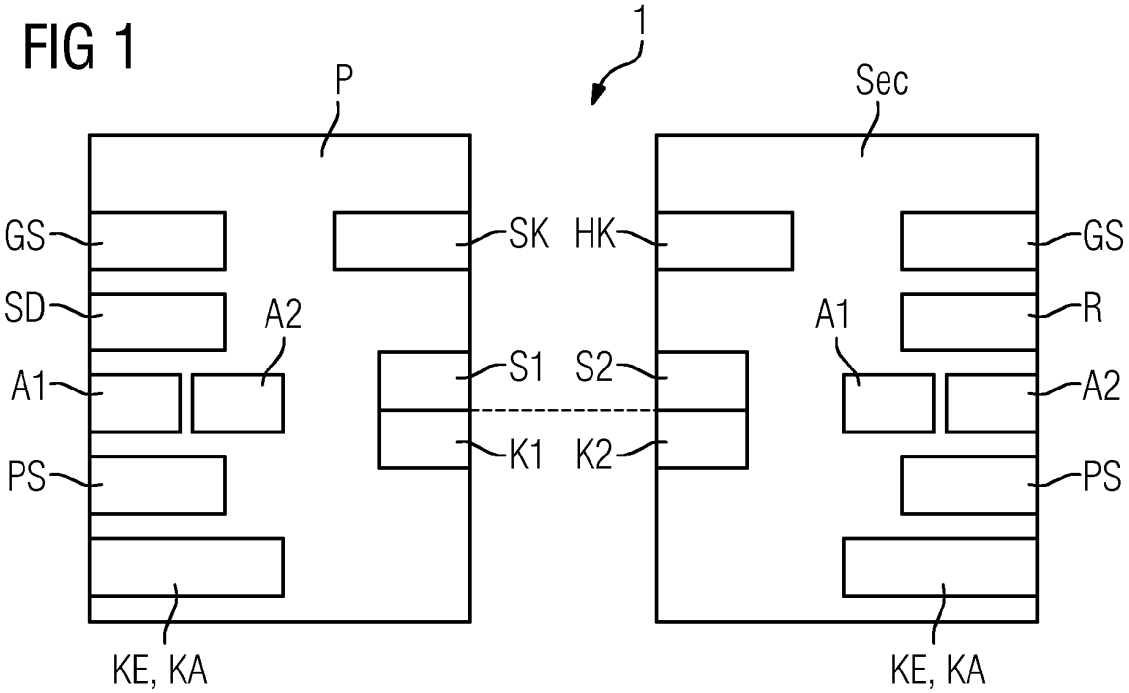
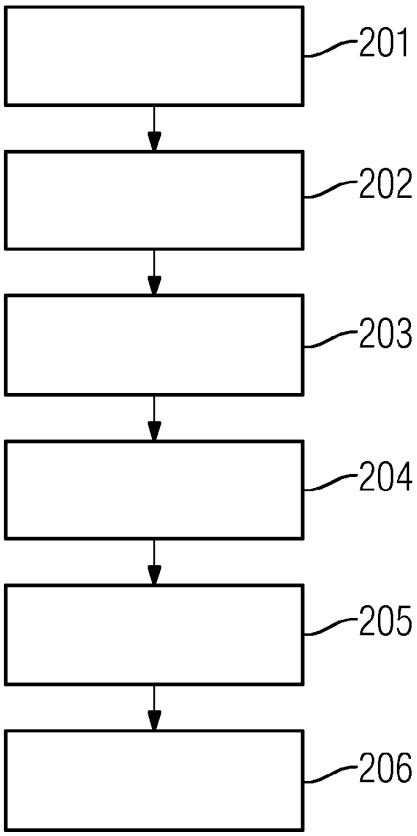

1
P
Sec
GS
SD
A1
PS
SK
HK
A2
S1
S2
K1
K2
GS
R
A1
A2
PS
KE, KA
KE, KA

FIG 2


201
202
203
204
205
206