(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 755 041**

(51) Int. CI.:

G06F 21/51 (2013.01)
G06F 21/57 (2013.01)
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.05.2016 PCT/EP2016/062243**

(87) Fecha y número de publicación internacional: **12.01.2017 WO17005410**

(96) Fecha de presentación y número de la solicitud europea: **31.05.2016 E 16727158 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2019 EP 3286872**

(54) Título: **Obtención de una clave criptográfica específica de un aparato a partir de una clave intersistemas para un aparato**

(30) Prioridad:

07.07.2015 DE 102015212657

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.04.2020

(73) Titular/es:

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

(72) Inventor/es:

ASCHAUER, HANS;
FALK, RAINER y
MERLI, DOMINIK

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Obtención de una clave criptográfica específica de un aparato a partir de una clave intersistemas para un aparato

La invención se refiere a un procedimiento así como a un aparato para obtener con aseguramiento una clave criptográfica específica de un aparato a partir de una clave intersistemas para un aparato, así como a un producto de programa de computadora con un programa de computadora, que presenta medios para realizar el citado procedimiento. Para ello se forma y se sella al menos una información de identificación del sistema específica del aparato durante una ejecución de un código de arranque (boot).

Los sistemas de computadoras, como en particular los sistemas embebidos o los llamados embedded systems, utilizan claves criptográficas para distintas finalidades de aplicación, como por ejemplo autentificación de un aparato, comunicación segura, comprobación de integridad, comprobación de licencia o protección del know how. Para ello es necesario obtener una clave criptográfica con aseguramiento.

Existen diversas soluciones basadas en software o soluciones para plataformas de hardware, como por ejemplo la memorización en un módulo de memoria de configuración, métodos de criptografía White box (de caja blanca), chips de módulos de plataforma de confianza (trusted plattform module) para PCs, criptocontroladores especialmente protegidos o memorias seguras (secure memories). Para simplificar procesos de fabricación, se utilizan entonces en la práctica claves idénticas en varios aparatos. Éstas pueden estar contenidas por ejemplo en una imagen de firmware de una unidad central del procesador, abreviadamente CPU o en un bitstream (cadena de bits) de un equipo de hardware programable o de un FPGA o bien estar archivadas en un módulo de memoria.

Se conoce en general la utilización de funciones de derivación de claves, como por ejemplo HMAC, SHA256 o HKDF, AES, etc., para calcular a partir de una clave criptográfica, en función de un parámetro de derivación, una clave derivada. Entonces es a menudo difícil archivar con aseguramiento una clave maestra (master key) existente.

Se conoce la forma de garantizar la seguridad de una masterkey o de una clave criptográfica derivada mediante un anclaje de hardware. Evidentemente a menudo no puede realizarse un anclaje de hardware o es caro y costoso.

El documento US 2015/180654 A1 describe un procedimiento para la obtención asegurada de una clave con una unidad de solicitud y una unidad de obtención. Entonces se deriva una clave a partir de parámetros de los cuales al menos uno lo utiliza la unidad de solicitud de manera impredecible para la derivación de claves. El parámetro impredecible puede estar unido a una plataforma de hardware. Además puede generarse la clave una sola vez durante cada proceso de arranque, al resultarle posible a un parámetro la activación por una sola vez durante el proceso de arranque.

Partiendo de esta base, consiste el objetivo de la presente invención en proporcionar un procedimiento, un producto de programa de computadora, así como un equipo que puedan proporcionar en uno o varios aparatos diferentes una clave criptográfica individual del aparato asegurada derivada de una clave intersistemas.

Este objetivo se logra mediante las características de las reivindicaciones independientes. Ventajosas variantes de configuración se indican en las reivindicaciones dependientes.

La invención se refiere a un procedimiento según la reivindicación 1, en particular para la obtención asegurada de una clave criptográfica específica de un aparato a partir de una clave intersistemas para un aparato, con las siguientes etapas:

- formación de varias informaciones de identificación del sistema específicas del aparato durante una fase de arranque, incluyendo las informaciones de identificación del sistema específicas del aparato varias partes, que se determinan y configuran por etapas;
- sellado de las informaciones de identificación del sistema específicas del aparato escribiendo, lo cual es posible en cada caso como máximo una sola vez, la respectiva información de identificación del sistema específica del aparato durante la fase de arranque o bien otra fase de arranque posterior;
- determinación de la clave intersistemas;
- derivación de la clave criptográfica específica del aparato a partir de la clave intersistemas utilizando las informaciones de identificación del sistema específicas del aparato;

formándose y sellándose al menos dos informaciones de identificación del sistema específicas del aparato durante la fase de arranque o la otra fase de arranque, sellándose en varias fases de arranque una respectiva información de identificación del sistema y

formándose una información completa de identificación del sistema específica del aparato y definitiva a partir de las informaciones de identificación del sistema como parámetro.

Bajo una clave intersistemas se entiende en la presente solicitud una clave del sistema o una clave maestra, que en particular es idéntica para ejemplares de aparato de idéntico firmware.

Bajo un aparato se entiende en lo que sigue por ejemplo un System on Chip (sistema en un chip) o un sistema embebido, que presenta por ejemplo una lógica en hardware programable y un procesador. Para este aparato debe generarse una clave criptográfica específica del aparato, pudiendo introducirse cualquier curva característica del aparato en la clave criptográfica específica del aparato. Al respecto puede tratarse de características de hardware al igual que de especificidades de la forma de funcionamiento o de la integración en red o de una tarea o misión dentro de un sistema.

Bajo la información de identificación del sistema específica del aparato han de entenderse en particular bits o secuencias de bits que durante la ejecución de un código de arranque pueden determinarse por ejemplo para arrancar o boot un sistema de computadora con bootlader (gestor de arranque). Bajo la fase de arranque se entiende en particular la fase del boot. El arranque se realiza mediante al menos una fase de arranque o el llamado boot-stage (fase de arranque). En el mismo puede cargarse y ejecutarse un Root File System (sistema de archivo raíz) temporal.

La información de identificación del sistema específica del aparato se configura o escribe tal que la misma ya no puede modificarse durante el siguiente funcionamiento en marcha. Esta configuración o escritura puede también denominarse sellado. Entonces es posible una escritura como máximo una sola vez durante una fase de arranque. También puede decirse que sólo es posible un acceso de escritura. En el siguiente funcionamiento en curso ya no puede modificarse el valor sellado y ya no puede escribirse de nuevo. Sólo cuando tiene lugar un siguiente arranque del sistema puede el mismo escribirse de nuevo. Esto tiene la ventaja de que la información de identificación del sistema específica del aparato sólo puede configurarse durante un arranque del sistema. Con preferencia se configura con cada arranque del sistema la ventana de tiempo disponible para el ataque es por lo tanto reducida, ya que durante el funcionamiento en curso del aparato no es posible ninguna modificación. Un atacante sólo puede realizar a menudo difícilmente una manipulación de una rutina de arranque del sistema, ya que allí se ejecuta un código de arranque fijo, que no puede cargarse a posteriori o que sólo puede actualizarse con una protección especial. Además durante la fase de arranque aún no existe a menudo ninguna conexión a red activa, con lo que tampoco son posibles ataques a través de una red de comunicación de datos.

En una variante se comprueba en un rearranque del aparato de qué forma se originó el rearranque. Así puede diferenciarse por ejemplo entre un power-on-reset (reinicio de encendido), un hardware-reset, un software-restart (rearranque). Una reconfiguración de la información de identificación del sistema específica del aparato sólo puede liberarse entonces por ejemplo cuando se realiza un power-on-reset o un hardware-reset mediante un pulsador local. En un software-reset o bien rearranque por el contrario puede permanecer activado el valor previamente configurado y tampoco puede modificarse mediante el código de arranque.

Además es posible bloquear la posibilidad de escritura de la información de identificación del sistema específica del aparato automáticamente incluso sin que se haya realizado un proceso de escritura cuando existe un criterio de bloqueo. Son criterios de bloqueo posibles un time-out (tiempo expirado), la configuración de una unidad de gestión de la memoria (Memory Management Unit, MMU) el acceso a un medio de memoria externo (por ejemplo. SD-Card) o la activación de una interfaz de red. Entonces no puede formarse ni configurarse ninguna clave criptográfica específica del aparato a partir de la clave intersistemas. Alternativamente puede configurarse automáticamente un valor sustitutivo fijo o valor por defecto como información de identificación del sistema.

La clave intersistemas puede determinarse por ejemplo eligiendo la misma a partir de una memoria interna o de una memoria realizada mediante una función que no puede clonarse físicamente. La clave criptográfica específica del aparato se deriva finalmente a partir de la clave intersistemas utilizando la información de identificación del sistema, de las que al menos hay una.

La información de identificación del sistema específica del aparato se utiliza por ejemplo como parámetro de derivación de claves para una función de derivación de claves. En las siguientes fases de ejecución no puede activarse ninguna otra información que pudiera sustituir la información de identificación del sistema específica del aparato.

Mediante el procedimiento descrito se evitan manipulaciones en las cuales se forma una clave en un aparato existente para otro aparato. Puesto que en ese momento la información de identificación del sistema específica del aparato interviene en la derivación de claves, sólo está individualizada la clave derivada en el hardware existente. Por ejemplo sólo puede formarse un desencriptado de datos en un

System on Chip con la clave específica para el correspondiente aparato. Una clave derivada en el aparato para otro aparato, queda así inválida.

Según una variante de configuración, se forma la información de identificación del sistema específica de un aparato utilizando un parámetro característico del aparato, como es en particular un número de serie o un tipo de un módulo de memoria o de un módulo periférico del aparato o utilizando un identificador de un procesador o un chip del aparato o utilizando una dirección MAC de un adaptador de red o un número de serie de un disco duro del aparato o utilizando una función no clonable físicamente o una información de versión o un valor hash de firmware o de datos de configuración.

Como módulos de memoria puede pensarse en particular en memorias flash, memorias EEPROM, tarjetas de memoria SD o lápices USB. Como módulos periféricos sirven ventajosamente sensores y actuadores. Bajo un chip se entiende en particular un circuito integrado, por ejemplo el circuito integrado que sirve para realizar el FPGA.

Según una variante de configuración, se utiliza para formar la información de identificación del sistema específica del aparato un código de inicialización o un código de programa de un sistema de archivos raíz.

En un sistema de archivos (files) RAM temporal, inicial, por ejemplo bajo LINUX un Init RD o Init RAMFS, brevemente para sistema Initial Ram Root File (archivo raíz inicial RAM), puede estar contenido un código de programa para formar una información de identificación del sistema individual del aparato. Alternativamente puede formarse y activarse la información de identificación del sistema individual del aparato o una parte de la misma ya durante una fase de arranque más temprana o fase boot, por ejemplo mediante un Second Stage Boot Loader (cargador de arranque de segunda etapa), por ejemplo U-Boot o un First Stage Boot Loader (cargador de arranque de primera etapa), por ejemplo un código boot de una CPU soft, que se carga como parte de una cadena de bits FPGA.

Según una variante de configuración, se realiza el sellado mediante una memoria volátil, que puede escribirse una sola vez, por ejemplo un registro, que impide otro acceso de escritura, o mediante una configuración en la que una memoria se configura tras el sellado como no escribible.

Por ejemplo puede estar previsto en un System on Chip con hardware reconfigurarle un registro, que sólo permite un único proceso de acceso a escritura. Alternativamente puede configurarse un flag (bandera) o una Memory Management Unit (unidad de gestión de la memoria) tal que se impide un acceso a escritura adicional. Una Random Access Memory (memoria de acceso aleatorio), abreviadamente RAM, se configura por ejemplo como no escribible. Además puede escribirse la información de identificación del sistema específica del aparato en un registro de un procesador, por ejemplo de una unidad de procesador principal, abreviadamente CPU. Al igual que también en una variante basada en FPGA, el registro puede estar definido como no modificable. Esto se realiza por ejemplo mediante una Write Once Memory (memoria que puede escribirse una sola vez) o bloqueo de un acceso a memoria. Además puede escribirse la información de identificación del sistema específica del aparato en el caché de un procesador de una CPU y configurarse allí como bloqueado, por ejemplo mediante un procedimiento Cache Lock (bloqueo de caché).

Según una variante de configuración se elige como clave intersistemas una Security Key (clave de seguridad) o Master Key (clave maestra), en particular de un módulo de memoria o de una Firmware Image (imagen de firmware) de una unidad de procesador o de una cadena de bits de un módulo de hardware programable.

Según una variante de configuración se modifica para la derivación una función de derivación de claves en función de la información de identificación del sistema específica del aparato o bien interviene, para una función fija de derivación de claves, la información de identificación del sistema específica del aparato como parámetro de derivación.

Se utiliza por ejemplo una Boot Time Derivation Function (función de derivación del tiempo de arranque), en la que interviene la información de identificación del sistema específica del aparato como parámetro de derivación de claves. La clave específica del aparato derivada de la clave intersistemas se escribe por ejemplo en un registro de claves sobre un FPGA, un registro de CPU o una inscripción caché. Alternativa o adicionalmente se modifica un código de software para la derivación de claves en función de la información de identificación del sistema específica del aparato tal que el código de software calcula en función de la información de identificación del sistema específica del aparato una derivación de clave. Por ejemplo una implementación ofuscada mediante Whitebox-Cryptography de una función de derivación de claves, por ejemplo tablas look-up (de consulta) allí contenidas, puede modificarse y/o configurarse en función de la información de identificación del sistema específica del aparato. Así se individualiza el algoritmo de derivación de claves, en lugar de un parámetro entrante.

Según un perfeccionamiento, realiza la función de derivación de claves la derivación durante el tiempo de ejecución. Durante el funcionamiento regular, es decir, durante el tiempo de ejecución o el llamado runtime del sistema, pueden calcularse claves derivadas mediante una Runtime Key Derivation Function (función de derivación de clave del tiempo de ejecución), resultando en distintos sistemas claves diferentes. Al respecto se prescribe durante el tiempo de ejecución de la Runtime Key Derivation Function RTKDF un parámetro de derivación DP, para determinar una clave derivada del tiempo de ejecución DRK a partir de la clave intersistemas. Por ejemplo utiliza la implementación de la Runtime Key Derivation Function la información de identificación de claves específica del aparato archivado en un registro como parámetro de derivación o bien prescribe otro valor como parámetro de derivación.

La Runtime Key Derivation Function puede realizarse por ejemplo en un FPGA de un System on Chip.

Además es posible que la implementación de la Runtime Key Derivation Function utilice la clave del aparato derivada de la información de identificación del sistema específica del aparato como clave de entrada (input).

Según la invención, se sella al menos otra información de identificación del sistema específica del aparato durante la fase de arranque o la otra fase de arranque. Al respecto se crea durante dos o más fases de arranque consecutivas o fases del proceso de arranque o boot completo en cada caso una información de identificación del sistema específica del aparato. En particular se forma la información de identificación del sistema específica del aparato, es decir, la información de identificación del sistema específica del aparato completo y definitivo, a partir de varias informaciones de identificación como parámetro. Así pueden dificultarse manipulaciones del hardware, ya que una sustitución de un componente del sistema, por ejemplo de una memoria flash o de una EEPROM da lugar a que se forme una información de identificación del sistema específica del aparato diferente. Esto trae como consecuencia que se deriven distintas claves durante el tiempo de ejecución. Con ello no pueden realizarse desencriptaciones de datos del sistema original en un sistema manipulado. Por ejemplo puede formarse la información de identificación del sistema específica del aparato completa como concatenación de los parámetros individuales. Con preferencia se forma la información de identificación del sistema específica del aparato como un valor hash criptográfico de los parámetros concatenados. Alternativamente puede formarse una cadena de valores hash de los parámetros.

Según la invención se escribe en varias fases del proceso de arranque una respectiva información, que en respectivas fases de arranque posteriores o consecutivas en cada caso ya no puede modificarse. Estas informaciones escritas en varias fases de arranque forman conjuntamente la información de identificación del sistema específica del aparato.

La invención se refiere además a un producto de programa de computadora con un programa de computadora que presenta medios para realizar el procedimiento según una de las ejecuciones antes descritas, cuando el programa de computadora se ejecuta en un equipo controlado por programa.

Un producto de programa de computadora, como por ejemplo un medio de programa de computadora, puede proporcionarse o suministrarse por ejemplo como medio de memoria, como por ejemplo tarjeta de memoria, lápiz USB, CD-ROM, DVD o también en forma de fichero descargable de un servidor en una red. Esto puede realizarse por ejemplo en una red de comunicación inalámbrica mediante la transmisión de un fichero correspondiente con el producto de programa de computadora o el medio de programa de computadora. Como equipo controlado por programa procede en particular un equipo de control, como por ejemplo un microprocesador para una smartcard o similar. El procedimiento o el equipo pueden también implementarse con cableado fijo o en FPGAs configurables.

La invención se refiere además a un equipo según la reivindicación 9, en particular para proporcionar con aseguramiento una clave criptográfica específica del aparato a partir de una clave intersistemas para un aparato, que presenta:

- una primera unidad para formar varias informaciones de identificación del sistema específicas del aparato durante una fase de arranque;
- una segunda unidad para sellar las informaciones de identificación del sistema específicas del aparato, pudiéndose escribir las informaciones de identificación del sistema específicas del aparato durante la fase del arranque u otra fase de arranque siguiente en cada caso como máximo una sola vez, formándose y sellándose al menos dos informaciones de identificación del sistema específicas del aparato durante la fase de arranque o la otra fase de arranque, sellándose en varias fases de arranque en cada caso una información de identificación del sistema;
- una tercera unidad para determinar la clave intersistemas;
- una cuarta unidad para derivar la clave criptográfica específica del aparato a partir de la clave intersistemas utilizando las informaciones de identificación del sistema específicas del aparato, formándose una información de identificación del sistema específica del aparato completa y definitiva a partir de las informaciones de identificación del sistema como parámetro.

Las correspondientes unidades pueden estar implementadas mediante técnica de hardware y/o también mediante técnica de software. En una implementación mediante técnica de hardware puede estar constituida la correspondiente unidad como equipo o como parte de un equipo, por ejemplo como computadora o como microprocesador. En una implementación mediante técnica de software puede estar constituida la correspondiente unidad 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.

La invención se describirá a continuación más en detalle en base a ejemplos de ejecución con la ayuda de las figuras. En las figuras se han dotado elementos que tienen la misma función de las mismas referencias, siempre que no se indique otra cosa. Se muestra en:

figura 1 una representación esquemática de un System on Chip para generar una clave criptográfica específica del aparato durante una fase de arranque;
figura 2 una representación esquemática de un System on Chip para utilizar una clave criptográfica específica del aparato durante el funcionamiento;
figura 3 una representación esquemática de un System on Chip para derivar una clave criptográfica específica del aparato en una fase de arranque según otra forma de ejecución de la invención;
figura 4 una representación esquemática de un System on Chip para utilizar una clave criptográfica específica del aparato según otro ejemplo de ejecución de la invención;
figura 5 una representación esquemática de un System on Chip para generar una clave criptográfica específica del aparato con varios parámetros configurados en el proceso de arranque para formar la información de identificación del sistema específica del aparato.

Los ejemplos de ejecución se describirán en base a un System on Chip SoC basado en FPGA. Al respecto puede tratarse de una lógica de hardware FPGA programable con una unidad CPU de Soft-Core-Processor (procesador de núcleo blando), por ejemplo una NIOS 2 sobre Altera Cyclone IV ó Cyclone V, o bien un Microblaze sobre Xilinx Kintex-7, Virtex-7 o Artix-7, o un System on Chip basado en FPGA con Hard-CPU como un ARM Core, por ejemplo Xilinx Zynq o Altera Cyclone V SoC.

La figura 1 muestra la estructura esquemática de un System on Chip SoC con componentes elegidos para los ejemplos de ejecución. Sobre un procesador CPU, por ejemplo una Soft-CPU o una Hard-CPU se arranca un sistema embebido con un sistema operativo basado en un Linux-Kernel (núcleo de software Linux), es decir, un llamado embedded LINUX. Sobre el System on Chip SoC está previsto, como procedimiento criptográfico asimétrico, un procedimiento RSA. Durante el proceso boot (de arranque), se arranca tras las fases de arranque iniciales un segundo Stage Boot Loader, por ejemplo U-Boot. Éste contiene una clave pública RSA, para verificar la firma digital del kernel y del sistema inicial Root File basado en RAM, creada mediante la correspondiente clave privada. Una imagen cargada sólo se acepta cuando presenta una firma RSA correcta.

Si es éste el caso, entonces se carga el kernel y se carga el Root-File-System inicial (Init RD) C2 basado en RAM. Se garantiza que se trata de un kernel auténtico y un File-System auténtico, es decir, de uno que no está manipulado. Una vez que el Second Stage Boot Loader ha cargado el sistema operativo kernel y el RAM-File-System C2 inicial, se arranca el kernel C3. El mismo ejecuta el código del programa (Init Code) C1, que está contenido en el File-System C2 inicial.

Durante este proceso de arranque, determina el código del programa C1 una información de identificación del sistema específica del aparato ID inequívoca y escribe la misma en el registro Boot Time System (sistema de tiempo de arranque) BTID. Este registro es un registro volátil, es decir, en un reset de hardware o en una interrupción de la corriente se pierde el contenido del registro volátil. No obstante, mediante medidas lógicas de protección queda asegurado que este registro sólo pueda escribirse una sola vez tras un reset de hardware. Esto se logra bien mediante una lógica interna de que sólo es posible la escritura una sola vez o bien activando una Write Only Flag (bandera de sólo escritura). Así no puede modificarse el valor del registro durante el tiempo de funcionamiento.

El código de programa o Bootcode C1 capta, para formar la información de identificación del sistema ID, los siguientes parámetros o un subconjunto de los siguientes parámetros:

- Fabricante, modelo y número de serie de una memoria EEPROM de sólo lectura programable que puede borrarse eléctricamente,
- código del fabricante, modelo y número de serie de uno o varios módulos de memoria flash F,
- fabricante, modelo y número de serie de uno o varios módulos de memoria de acceso directo RAM,
- fabricante, modelo y número de serie de sensores S o actuadores A conectados mediante interfaces de Input/-Output (entrada/salida) IO,
- número de serie y dirección de red de un adaptador de red NW,
- fabricante, modelo y número de serie del System on Chip SoC.

Estos parámetros individuales de aparatos se captan, por ejemplo mediante módulos kernel o el listado de las interfaces para controlar el hardware, es decir, el sistema de ficheros dev. Ventajosamente se determinan parámetros protegidos criptográficamente, por ejemplo cuando la EEPROM es un módulo EEPROM secreto, que apoya una autentificación reto-respuesta.

Cuanto mayor sea el número de los citados parámetros que intervienen, tanto más complejo será por un lado, dado el caso, el cálculo, pero por otro lado tanto más segura será la derivación de claves que para un atacante se vuelve crecientemente opaca cuantas más dependencias específicas de aparatos existan.

Es posible que la información de identificación del sistema específica del aparato ID se escriba en varias partes. La información de identificación del sistema específica del aparato ID puede incluir varias partes, que se determinan y configuran paulatinamente. Entonces, mediante varias de las etapas siguientes, o mediante todas ellas, puede determinarse y configurarse una parte de la información de identificación del sistema específica del aparato:

- El First Stage Boot Loader puede determinar y configurar una información del sistema.
- El Second Stage Boot Loader, por ejemplo U-Boot, puede determinar y configurar una información del sistema. Esto puede realizarlo el propio U-Boot o bien un código de programa Boot o un Bootscript (programa de arranque), que es descargado por el U-Boot.
- El propio Linux-Kernel o bien un módulo kernel enlazado estáticamente puede determinar y configurar una información del sistema.
- Un módulo Linux-Kernel cargado a posteriori puede determinar y configurar una información del sistema.
- El código de programa de inicialización de Initrd o un código de programa descargado desde allí o un Script puede determinar y configurar una información del sistema.
- Un Startup-Script (programa de arranque) del sistema Linux arrancado tras enganchar (mounten) el sistema de ficheros, puede configurar una información del sistema.

En esta activación de la información de identificación del sistema específica del aparato en varias etapas se configura en cada caso la información de una etapa individual tal que la misma ya no puede modificarse al ejecutar las siguientes etapas.

La información de identificación del sistema específica del aparato ID determinada está compuesta en una variante por varios parámetros P1, P2, Pn y se concatena, es decir, se enganchan uno con otro y se escriben en el Boot Time System ID-Register BTID, es decir:

$$ID := P1 \| P2 \| Pn$$

Ventajosamente calcula el código de programa C1 un valor hash criptográfico mediante una función hash H de los parámetros determinados como información de identificación del sistema específica del aparato ID, es decir:

$$ID := H(P1 \| P2 \| Pn)$$

Entonces se utiliza por ejemplo la función hash criptográfica SHA256 o Blake2.

En otra variante calcula el código de programa C1 un valor hash criptográfico de los parámetros determinados iterativamente encadenando las funciones hash, es decir:

$$ID := H(Pn \| H\big(P2 \| H(P1)\big) \ldots)$$

Puede utilizarse igualmente una Key Derivation Function como HMAC-SHA256 como función hash.

En el FPGA se ejecuta, a partir de una clave intersistemas SK, que por ejemplo está archivada igualmente en una EEPROM instalada, e incluyendo la información de identificación del sistema específica del aparato ID, una función de derivación de claves KDF. El resultado de la ejecución es la clave criptográfica específica del aparato.

La figura 2 muestra la situación del System on Chip basado en FPGA de la figura 1 durante un funcionamiento normal. Como función de derivación de claves está prevista una Runtime Key Derivation Function RTKDF. Las aplicaciones APP1 o APP2, que se ejecutan sobre el procesador CPU, recurren a una función de la Runtime Key Derivation Function RTKDF para, independientemente de un parámetro de derivación Runtime Derivation Parameter RTDP que puede elegirse durante el tiempo de funcionamiento, obtener una clave del tiempo de funcionamiento RTIDK derivada. Ésta es la clave criptográfica específica del aparato, que en este ejemplo se forma durante el tiempo de funcionamiento. Entonces pueden formarse varias claves del tiempo de funcionamiento distintas para finalidades diferentes, por ejemplo

para desencriptar un fichero o para abrir una memoria de claves o para montar un sistema de ficheros encriptado o para desencriptar partes integrantes de un código.

En la derivación de claves interviene regularmente también la información inequívoca de identificación del sistema específica del aparato ID del Boot Time System Identifier-Register BTID. Este valor está memorizado en el registro que se escribió durante el proceso de arranque. Además de ello, interviene regularmente la clave intersistemas SK como clave maestra.

En la figura 3 se representa una variante en la que está prevista una Boot Time Key Derivation Function BTKDF en la lógica programable FPGA, que en función de una información de identificación del sistema específica del aparato ID configurada como Boot time System-ID BTSID, deriva una Runtime Key RTK a partir de una clave del sistema SK.

En la figura 4 se representa la utilización de la Runtime Key RTK mediante la Runtime Key Derivation Function RTKDF, interviniendo una Runtime Key RTK formada tal como se describió en la figura 3 juntamente con un parámetro de derivación de Runtime RTDP en la Runtime Key Derivation Function RTKDF. La RTIDK criptográfica específica del aparato así derivada, formada durante el tiempo de funcionamiento, es utilizada por el procesador CPU sobre demanda.

La figura 5 muestra esquemáticamente un System on Chip SoC, en el que el Boot Time System-ID o la información de identificación del sistema específica del aparato incluye varias partes, que se configuran en cada caso separadamente. En el ejemplo representado está compuesta la información de identificación del sistema específica del aparato por tres parámetros parciales ID1, ID2 e ID3, que se escriben en respectivos registros BTID1, BTID2, BTID3. Los tres parámetros parciales son configurados en el ejemplo representado por el First Stage Boot Loader 1SBL y por el Second Stage Boot Loader 2SBL y por el código de programa del sistema de archivos Initrd C1.

El valor configurado resulta así como valor compuesto, concatenado, de los valores ID1, ID2 e ID3. En una variante sólo es posible una derivación de claves mediante la Runtime Key Derivation Function RTKDF cuando los tres parámetros están configurados. En otra variante es posible una derivación de claves incluso ya durante la fase de arranque, interviniendo las partes ya configuradas en la derivación de claves. En esta variante interviene ventajosamente otro parámetro en la derivación de claves, que se forma en función de qué partes del registro Boot Time System ID ya están configuradas o aún no están configuradas.

Resultan en particular ventajas para escenarios en los que un circuito integrado utilizado no presenta ningún número de serie interno inequívoco. Si no contiene el módulo hardware utilizado ningún número de serie de chip inequívoco, entonces resulta por ejemplo una clave generada mediante una cadena de bits FPGA, con clave maestra allí incluida, idéntica en distintos circuitos integrados.

Mediante el procedimiento descrito y el equipo descrito en la presente solicitud, se logra una individualización del chip muy compleja de manipular. La misma puede realizarse simplemente en software. Las manipulaciones de hardware de un sistema se ven dificultadas, ya que por ejemplo la sustitución de un componente da lugar a una modificación de la información de identificación del sistema específica del aparato. Así se derivan distintas claves durante el tiempo de funcionamiento. Así se impiden ventajosamente desencriptaciones de ficheros del sistema original en un sistema manipulado.

Aun cuando la invención se ha ilustrado y descrito más en detalle mediante los ejemplos de ejecución, no queda limitada la invención por los ejemplos dados a conocer y el especialista puede deducir a partir de los mismos otras variaciones sin abandonar el ámbito de protección de la invención.

REIVINDICACIONES

1. Procedimiento para la obtención asegurada de una clave criptográfica específica de un aparato (IDK) a partir de una clave intersistemas (SK) para un aparato, con las siguientes etapas:
   - formación de varias informaciones de identificación del sistema específicas del aparato (ID1, ID2) durante al menos dos fases de arranque consecutivas, incluyendo las informaciones de identificación del sistema específicas del aparato (ID1, ID2) varias partes, que se determinan y configuran por etapas;
   - sellado de las informaciones de identificación del sistema específicas del aparato (ID1, ID2) escribiendo, lo cual es posible en cada caso como máximo una sola vez, la respectiva información de identificación del sistema específica del aparato (ID1, ID2) durante las fases de arranque, de las que al menos hay dos;
   - determinación de la clave intersistemas (SK);
   - derivación de la clave criptográfica específica del aparato (IDK) a partir de la clave intersistemas (SK) utilizando una información de identificación del sistema específica del aparato (ID);

   en el cual se forman y sellan al menos dos informaciones de identificación del sistema específicas del aparato (ID1, ID2) durante las fases de arranque, de las que al menos hay dos, sellándose en las fases de arranque, de las que al menos hay dos, una de las informaciones de identificación del sistema (ID1, ID2) y
   formándose la información completa y definitiva de identificación del sistema específica del aparato (ID) a partir de las informaciones de identificación del sistema (ID1, ID2) como parámetro.

2. Procedimiento según la reivindicación 1,
   en el que se forman las informaciones de identificación del sistema específicas de un aparato (ID1, ID2) utilizando un parámetro característico del aparato, como es en particular un número de serie o un tipo de un módulo de memoria o de un módulo periférico del aparato o utilizando un identificador de un procesador o un chip del aparato o utilizando una dirección MAC de un adaptador de red o un número de serie de un disco duro del aparato o utilizando una función no clonable físicamente o una información de versión o un valor hash de firmware o de datos de configuración.

3. Procedimiento según la reivindicación 1 ó 2,
   en el que para formar las informaciones de identificación del sistema específicas de un aparato (ID1, ID2), se utiliza un código de inicialización o un código de programa de un sistema de archivos raíz (IFS).

4. Procedimiento según una de las reivindicaciones precedentes,
   en el que se realiza el sellado
   - mediante una memoria volátil, que puede escribirse una sola vez, por ejemplo un registro, que impide otra escritura adicional, o
   - mediante una configuración en la que una memoria se configura tras el sellado como no escribible.

5. Procedimiento según una de las reivindicaciones precedentes,
   en el que como clave intersistemas (SK) se elige una Secret Key o Master Key, en particular de un módulo de memoria o de una Firmware Image de una unidad de procesador o de una cadena de bits de un módulo de hardware programable.

6. Procedimiento según una de las reivindicaciones precedentes,
   en el que para la derivación se modifica una función de derivación de claves en función de la información de identificación del sistema específica de un aparato (ID1, ID2) o bien intervienen, para una función fija de derivación de claves, las informaciones de identificación del sistema específicas del aparato (ID1, ID2) como parámetro de derivación.

7. Procedimiento según la reivindicación 6,
   en el que la función de derivación de claves ejecuta la derivación durante el tiempo de funcionamiento.

8. Producto de programa de computadora con un programa de computadora que presenta medios para realizar el procedimiento según una de las reivindicaciones 1 a 7, cuando el programa de computadora se lleva, para su ejecución, a un equipo controlado por programa.

9. Equipo para proporcionar con aseguramiento una clave criptográfica específica del aparato (IDK) a partir de una clave intersistemas (SK) para un aparato, que presenta:
   - una primera unidad para formar varias informaciones de identificación del sistema específicas del aparato (ID1, ID2) durante al menos dos fases de arranque consecutivas;
   - una segunda unidad para sellar las informaciones de identificación del sistema específicas del aparato (ID1, ID2), pudiéndose escribir las informaciones de identificación del sistema específicas

del aparato (ID1, ID2) durante las fases del arranque, de las que al menos hay dos, en cada caso como máximo una sola vez, formándose y sellándose al menos dos informaciones de identificación del sistema específicas del aparato (ID1, ID2) durante las fases de arranque, de las que al menos hay dos, sellándose en las fases de arranque, de las que al menos hay dos, en cada caso una de las informaciones de identificación del sistema (ID1, ID2);

- una tercera unidad para determinar la clave intersistemas (SK);
- una cuarta unidad para derivar la clave criptográfica específica del aparato (IDK) a partir de la clave intersistemas utilizando una información de identificación del sistema específica del aparato, formándose una información de identificación del sistema específica del aparato completa y definitiva (ID),

formándose la información de identificación del sistema específica del aparato completa y definitiva (ID) a partir de las informaciones de identificación del sistema (ID1, ID2) como parámetro.

FIG 1

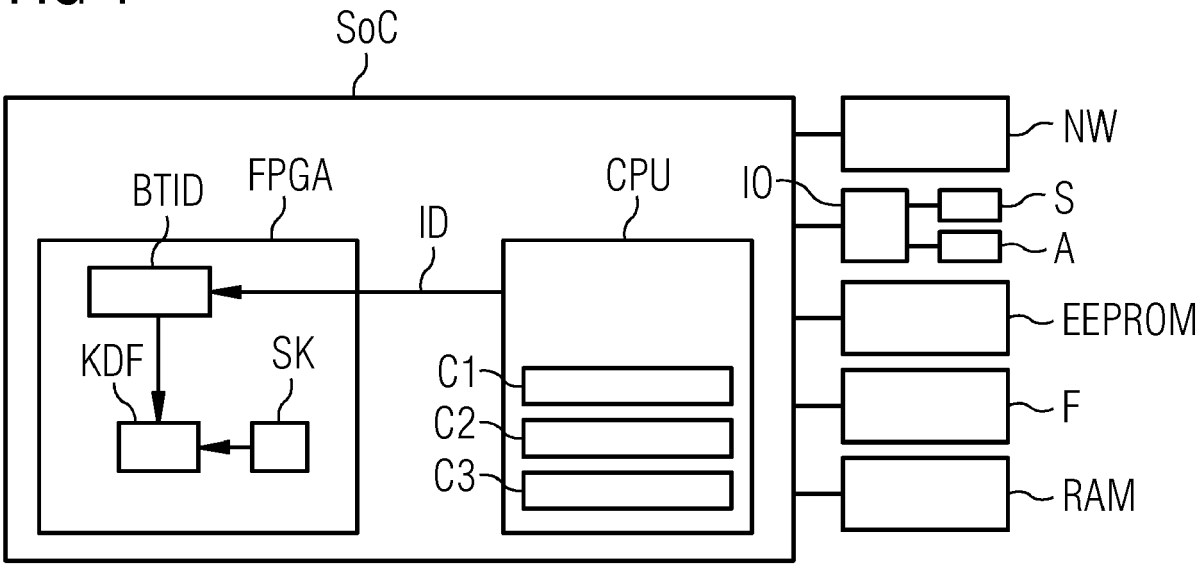

SoC
BTID
FPGA
ID
CPU
IO
NW
S
A
EEPROM
F
RAM
KDF
SK
C1
C2
C3

FIG 2

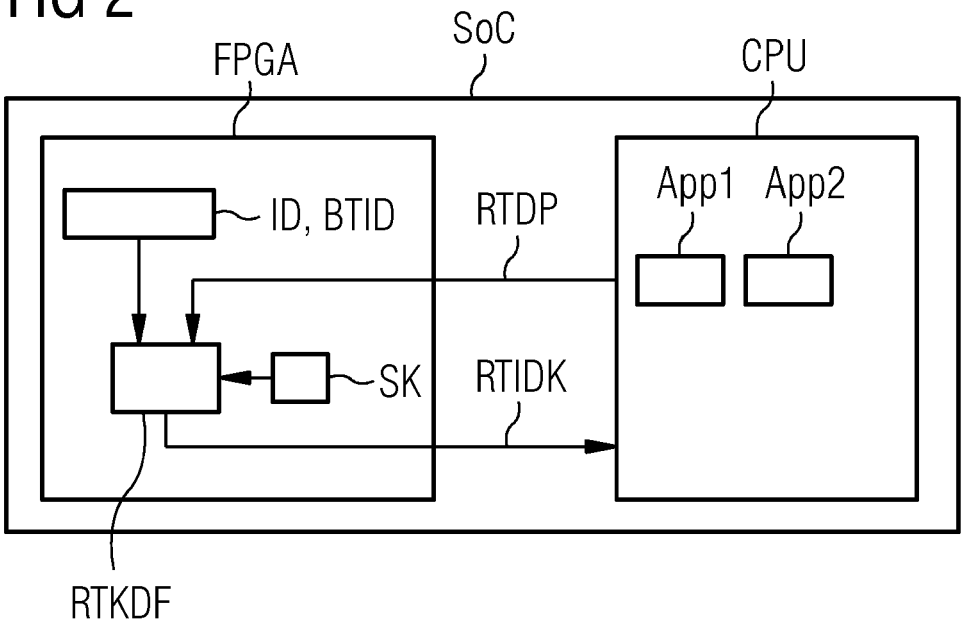

SoC
FPGA
CPU
ID, BTID
RTDP
App1
App2
SK
RTIDK
RTKDF

FIG 3

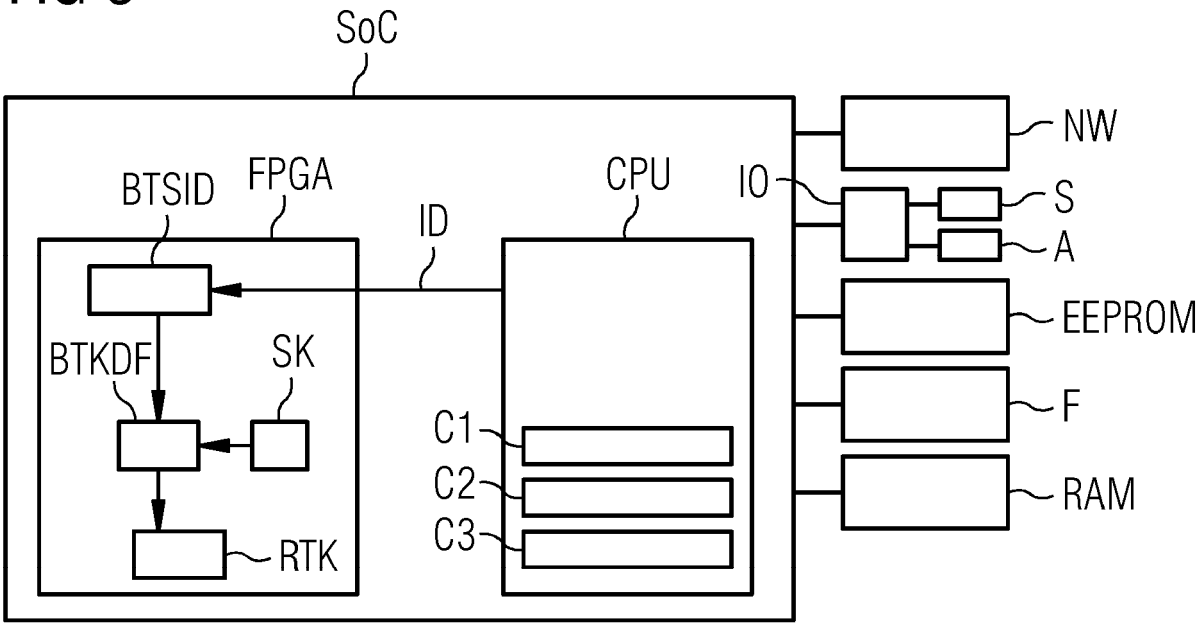

SoC
BTSID
FPGA
ID
CPU
IO
NW
S
A
EEPROM
F
RAM
BTKDF
SK
RTK
C1
C2
C3

FIG 4

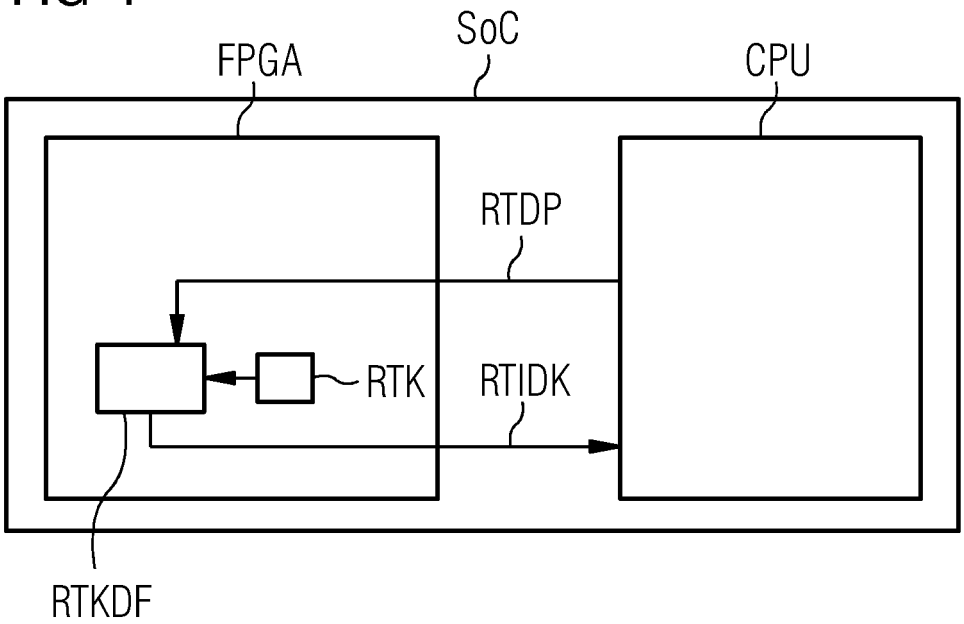
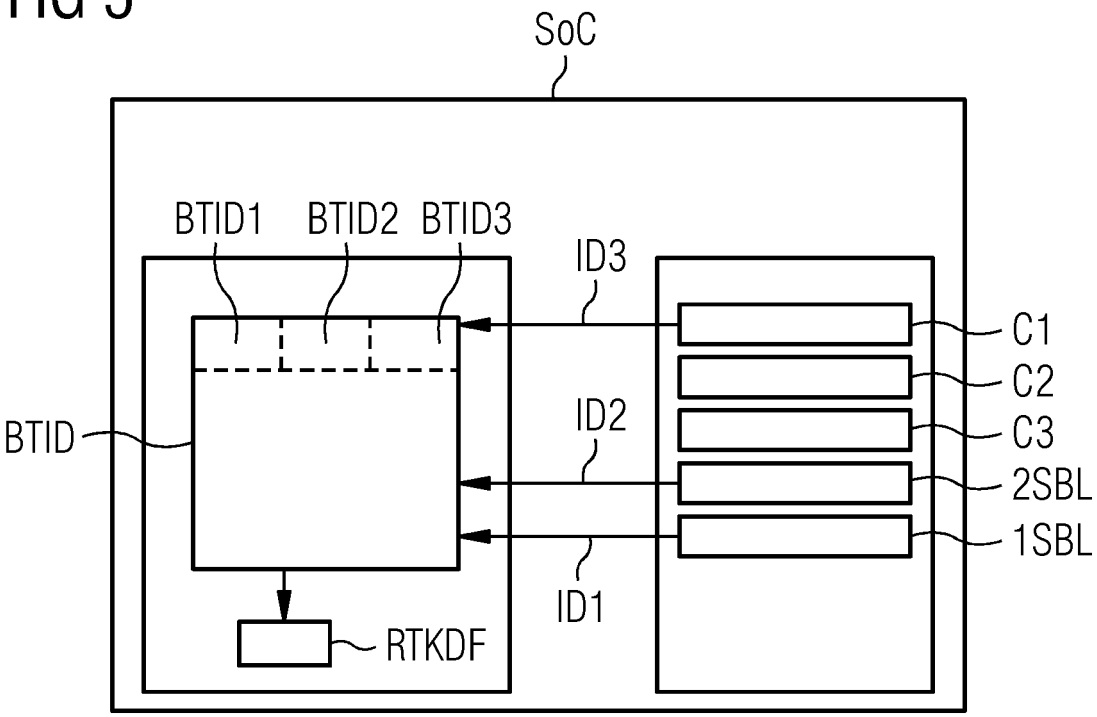

SoC
FPGA
CPU
RTDP
RTK
RTIDK
RTKDF

FIG 5


SoC
BTID1
BTID2
BTID3
ID3
C1
C2
C3
BTID
ID2
2SBL
1SBL
ID1
RTKDF