(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 117**

(51) Int. CI.:

G06F 21/00 (2013.01)
G06F 21/10 (2013.01)
G06F 21/57 (2013.01)
G06F 21/73 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.02.2012 PCT/EP2012/000534**

(87) Fecha y número de publicación internacional: **16.08.2012 WO12107200**

(96) Fecha de presentación y número de la solicitud europea: **06.02.2012 E 12702770 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.12.2018 EP 2673731**

(54) Título: **Procedimiento para la programación de un chip de terminal móvil**

(30) Prioridad:

08.02.2011 DE 102011010627

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.04.2019

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

SPITZ, STEPHAN;
DIETZE, CLAUS y
GALKA, GERO

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento para la programación de un chip de terminal móvil

La invención se refiere a un procedimiento para la programación de un chip de terminal móvil, a un procedimiento para la activación de un sistema operativo de seguridad utilizando el procedimiento para la programación y un procedimiento para la configuración asegurada de un terminal móvil que contiene un chip utilizando el procedimiento para la programación.

Los terminales móviles, tal como, por ejemplo, teléfonos móviles, teléfonos inteligentes y similares contienen un chip (chip de microprocesador) con un circuito integrado (IC = *Integrated Circuit*), también denominado SoC (*System on Chip*), mediante el que se controla el terminal móvil incluyendo sus componentes, tal como, por ejemplo, la pantalla, el teclado, el lector de tarjetas para tarjetas SIM y/u otras tarjetas.

El chip se fabrica por parte de un fabricante de chips (también denominado *SoC Provider*, SoCP), se proporciona a un fabricante de terminales diferente del fabricante de chips (también denominado *Original Equipment Manufacturer* OEM), y se programa por parte del fabricante de terminales con un sistema operativo (es decir, se programa un sistema operativo en el chip) y se incorpora a un terminal móvil. El sistema operativo para el chip se genera por regla general no por parte del fabricante de terminales, sino por parte del fabricante de chips o un creador de sistemas operativos asociado con el fabricante de chips. Sin embargo, dado que en el sistema operativo deben tenerse en cuenta particularidades del terminal móvil, para el que está previsto el chip, el sistema operativo no se programa al momento por parte del fabricante de chips, sino por parte del fabricante de terminales en el chip. Entre la fabricación del chip y el suministro del chip al fabricante de terminales se llevan a cabo por regla general, por parte del fabricante de chips y/o por empresas asociadas con el fabricante de chips, etapas de programación, que sin embargo no forman parte del objeto de la presente solicitud de patente.

Mediante la programación del chip fuera del campo de acción del fabricante de chips existe un riesgo de que se proporcionen chips falsificados, denominados a menudo chips “grises”, al fabricante de terminales, que no proceden del fabricante de chips y que posiblemente tienen propiedades distintas a las de los chips originales del fabricante de chips. Sin embargo, el fabricante de terminales está interesado en implementar chips originales del fabricante de chips con propiedades garantizadas en sus terminales móviles. El fabricante de chips está a su vez interesado en que el sistema operativo previsto para sus chips se programe solo en sus chips, pero no en chips de otra procedencia.

Según el estado actual, para defenderse contra chips grises se programan en el fabricante de chips números de serie en los chips. Antes de que en el fabricante de terminales se programen en un chip datos adicionales, tales como, por ejemplo, el sistema operativo, se comprueba el número de serie del chip. Por medio de listas de números de serie, en las que están apuntados todos los números de serie válidos, el fabricante de terminales puede reconocer si el chip tiene un número de serie válido. Los chips sin números de serie válidos no se programan. El documento WO03073688 da a conocer un procedimiento en el que se programa un número de serie en el chip.

Las listas de números de serie pueden ser muy extensas, lo que hace que su manipulación sea laboriosa y complicada. Además, la transmisión segura de las listas de números de serie entre el fabricante de chips y el fabricante de terminales y eventualmente partes adicionales significa un gran esfuerzo.

Por parte del solicitante de la presente solicitud de patente se fabrica y se comercializa bajo la marca MOBICORE un sistema operativo de seguridad para chips que deben implementarse en terminales (de telefonía) móviles (por ejemplo, teléfonos móviles, teléfonos inteligentes). Las aplicaciones críticas en cuanto a la seguridad y algunas funciones del sistema (por ejemplo, controlador de teclado) se controlan de manera segura mediante el sistema operativo de seguridad MOBICORE. Aplicaciones adicionales y otras funciones del sistema (por ejemplo, actualmente el controlador de pantalla) se controlan mediante un sistema operativo normal que existe además del sistema operativo de seguridad. El sistema operativo de seguridad comprende una clave criptográfica, la clave de autenticación Kauth, por medio de la que puede identificarse el sistema operativo de seguridad con respecto a un sistema de fondo. Opcionalmente, la clave de autenticación Kauth está prevista además para hacer funcionar un canal de comunicación seguro entre el chip o el terminal móvil y el sistema de fondo. El sistema de fondo es, por ejemplo, un sistema de fondo en sí conocido de una red de telefonía móvil.

La invención se basa en el objetivo de crear un procedimiento eficaz y seguro para la programación de un chip de terminal móvil, en el que la programación se permita solo como mucho para chips de origen predeterminado. En particular, pretende crearse un procedimiento de este tipo, que funcione sin listas de números de serie. Además, según perfeccionamientos de la invención pretende indicarse un procedimiento para la activación de un sistema operativo de seguridad y un procedimiento para la configuración asegurada de un terminal móvil que contiene un chip, en cada caso utilizando el procedimiento para la programación.

El objetivo se alcanza mediante un procedimiento según la reivindicación 1. Configuraciones ventajosas de la invención se indican en las reivindicaciones dependientes.

El procedimiento según la reivindicación 1 está configurado para la programación de un chip para un terminal móvil. A este respecto, en una etapa preparatoria se programa un número de serie en el chip. A continuación, se verifica en una etapa de programación el número de serie y, solo en el caso de que se haya verificado satisfactoriamente el número de serie, se realiza una programación de al menos un dato adicional en el chip. El procedimiento se caracteriza porque el número de serie puede verificarse por medio de un módulo de seguridad, usando una información secreta almacenada en el módulo de seguridad, que es diferente del número de serie. A este respecto, por el "dato adicional" se entiende cualquier tipo de datos, por ejemplo, código de programa (por ejemplo, un sistema operativo, véase más adelante) o datos individuales (por ejemplo, una clave (de autenticación) criptográfica), que están previstos para ejecutarse conjuntamente con el código de programa.

Dado que el número de serie puede verificarse usando la información secreta almacenada en el módulo de seguridad, para la verificación del número de serie se requiere únicamente el módulo de seguridad pero ninguna lista de números de serie. Por consiguiente, el procedimiento es al menos igual de seguro que un procedimiento con una comprobación de números de serie por medio de listas de números de serie, pero esencialmente más eficaz, dado que no tiene que manipularse ninguna lista de números de serie.

La invención se da a conocer en las reivindicaciones adjuntas. Por tanto, según la reivindicación 1 se crea un procedimiento eficaz y seguro para la programación de un chip de terminal móvil con comprobación de origen para el chip.

Opcionalmente, en respuesta a la verificación satisfactoria del número de serie se programa en el chip el dato adicional por medio del módulo de seguridad directamente y sin posibilidad de intervención desde fuera del módulo de seguridad. De este modo se consigue que tras la verificación satisfactoria del número de serie se asigne el dato adicional exclusivamente al chip, cuyo número de serie acaba de verificarse, y pueda programarse en el mismo. Por el contrario, un cambio del chip por otro chip tras la verificación del número de serie y antes de la programación del dato adicional en el chip no es posible. Por consiguiente, se garantiza que solo se programe el dato adicional en chips de origen correcto.

Opcionalmente, el número de serie se verifica reproduciendo, es decir, generando de nuevo, el número de serie o una información dependiente del número de serie usando la información secreta. En el segundo caso se programa en el chip la información dependiente del número de serie en la etapa preparatoria, preferiblemente de manera adicional.

Según una primera forma de realización, el número de serie se forma mediante una regla de asignación y la regla de asignación está almacenada como información secreta en el módulo de seguridad. En este caso, para la verificación del número de serie, se lee del chip el número de serie por medio del módulo de seguridad, se genera de nuevo el número de serie por medio de la regla de asignación almacenada en el módulo de seguridad, se compara el número de serie leído y el generado de nuevo (preferiblemente también en el módulo de seguridad) y, en el caso de coincidencia, se considera el número de serie como verificado. La regla de asignación procesa datos de entrada, que, por ejemplo, pueden comprender un número aleatorio y datos adicionales, y genera a partir de esto el número de serie.

Según una segunda forma de realización, además del número de serie se almacena en el chip una firma digital formada usando el número de serie y una clave secreta y la clave secreta se almacena como información secreta en el módulo de seguridad. En este caso, para la verificación del número de serie se leen del chip el número de serie y la firma digital por medio del módulo de seguridad, la firma se genera de nuevo en el módulo de seguridad por medio del número de serie leído y de la clave secreta almacenada en el módulo de seguridad, se comparan la firma leída y la generada de nuevo (preferiblemente también en el módulo de seguridad) y, en el caso de coincidencia de las firmas, se considera el número de serie como verificado.

Opcionalmente, la información secreta está almacenada en el módulo de seguridad de manera protegida frente a la lectura. Por ejemplo, una lectura directa de la información secreta no es posible o solo como mucho tras una autenticación satisfactoria con respecto al módulo de seguridad. La información secreta se usa dentro del módulo de seguridad para la verificación del número de serie del chip, sin salir del módulo de seguridad.

Opcionalmente, como dato adicional está previsto un sistema operativo de seguridad o al menos una parte de un sistema operativo de seguridad. Por ejemplo, en la etapa de programación, el sistema operativo de seguridad solo se programa en el chip en el caso en el que el número de serie se haya verificado satisfactoriamente.

Opcionalmente, como dato adicional está prevista una clave criptográfica necesaria para una funcionalidad de un sistema operativo de seguridad implementado o que debe implementarse todavía en el chip, por ejemplo, una clave de autenticación. El propio sistema operativo de seguridad se programa en el chip opcionalmente antes o después de la verificación del número de serie, o alternativamente en parte antes y en parte después. Opcionalmente, como dato adicional está prevista la clave de autenticación Kauth del sistema operativo de seguridad MOBICORE descrito al principio.

Opcionalmente, la clave criptográfica, por ejemplo, clave de autenticación, se genera en el módulo de seguridad, opcionalmente de manera directa en respuesta a la verificación satisfactoria del número de serie. La clave generada se programa a continuación en el chip, opcionalmente sin posibilidad de intervención desde fuera del módulo de seguridad.

Opcionalmente, la clave criptográfica se genera usando el número de serie. De este modo, la clave criptográfica depende del número de serie, y con ello la clave criptográfica es única, igual que el número de serie, para el chip.

Un procedimiento para la activación de un sistema operativo de seguridad se realiza mediante un procedimiento para la programación de un chip en el que, tal como se describió anteriormente, en la etapa preparatoria se programa el número de serie en el chip. Como dato adicional está prevista una clave criptográfica necesaria para una funcionalidad de un sistema operativo de seguridad, en particular una clave de autenticación. En el procedimiento para la activación del sistema operativo de seguridad se programa adicionalmente en el chip el sistema operativo de seguridad con la excepción de la clave criptográfica y de este modo se implementa en el chip. En la etapa de programación, la programación de la clave criptográfica en el chip se realiza solo en el caso de que el número de serie se haya verificado satisfactoriamente. Al programar la clave en el chip, se activa el sistema operativo de seguridad y por consiguiente es funcional a partir de esta operación de programación.

El procedimiento puede utilizarse de manera especialmente ventajosa en el caso de una programación de división de trabajo de un chip para un terminal móvil, estando dividida la programación del chip, por ejemplo, entre un fabricante de chips y un fabricante de terminales (por ejemplo, fabricante de terminales de telefonía móvil).

Opcionalmente, la etapa preparatoria se realiza por parte de un primer programador (por ejemplo, fabricante de chips) y la etapa de programación se realiza por parte de un segundo programador separado de manera lógica y/o espacial del primer programador (por ejemplo, fabricante de terminales). Dado que la verificación de los números de serie se produce sin listas de números de serie y únicamente requiere el módulo de seguridad, se suprime el intercambio, necesario hasta la fecha, de listas de números de serie entre el primer y el segundo programador, es decir, por ejemplo, entre el fabricante de chips y el fabricante de terminales.

Opcionalmente, la información secreta se programa por parte del primer programador (por ejemplo, fabricante de chips) en el módulo de seguridad y el módulo de seguridad la proporciona para la realización de la etapa de programación al segundo programador (por ejemplo, fabricante de terminales).

El módulo de seguridad está diseñado opcionalmente como sistema completo con un criptoprocesador, una memoria para información secreta y una unidad de control para la programación del chip. Opcionalmente, la memoria puede leerse exclusivamente mediante el criptoprocesador. El criptoprocesador está configurado para, usando información secreta almacenada en la memoria, realizar cálculos, por ejemplo, cálculos de firma, cálculos de número de serie según algoritmos, operaciones de comparación, generación de claves, en particular generación de una clave de autenticación Kauth para un sistema operativo de seguridad Mobicore. La unidad de control para la programación del chip está configurada para programar chips. Preferiblemente, el criptoprocesador y la unidad de control para la programación del chip están acoplados entre sí de tal manera que la programación de chip puede controlarse directamente mediante resultados de cálculo del criptoprocesador.

Según un primer perfeccionamiento de la invención, en la etapa de programación en el módulo de seguridad se genera un conjunto de datos de verificación que comprende al menos la información secreta, por medio del que puede verificarse el número de serie. El conjunto de datos de verificación se envía a un sistema de fondo. En una etapa de verificación que se encuentra, temporalmente, después de la etapa de programación se verifica de nuevo por medio del conjunto de datos de verificación el número de serie en el sistema de fondo, aceptándose el chip en el caso de que el número de serie se haya verificado satisfactoriamente en la etapa de verificación y rechazándose el chip en el caso de que el número de serie no se haya verificado satisfactoriamente en la etapa de verificación. La etapa de verificación se realiza, por ejemplo, con motivo del registro de un terminal móvil que contiene el chip en el sistema de fondo.

Opcionalmente, en el primer perfeccionamiento de la invención en la etapa de programación, como al menos una parte del conjunto de datos de verificación, se genera un dato de clave-número de serie dependiente de la clave y del número de serie, por ejemplo, al procesarse la clave y el número de serie por medio de un algoritmo G para dar el dato de clave-número de serie, y enviarse al sistema de fondo. En la etapa de verificación se verifica por medio del conjunto de datos de verificación, además del número de serie o en lugar del número de serie, el dato de clave-número de serie, por ejemplo, calculando una vez más el dato de clave-número de serie. Si es necesario, el conjunto de datos de verificación comprende el algoritmo G.

En un procedimiento según la invención para la configuración asegurada de un terminal móvil que contiene un chip para un sistema de telefonía móvil, según un segundo perfeccionamiento de la invención, en el chip se realiza una etapa preparatoria (que comprende en particular la programación del número de serie y dado el caso de la firma) y una etapa de programación (que comprende en particular la verificación del número de serie y dado el caso la

programación del dato adicional, por ejemplo la clave (de autenticación)), tal como se describió anteriormente. A continuación, se lleva el chip con un sistema de fondo del sistema de telefonía móvil a una conexión de intercambio de datos, para registrar el terminal móvil en el sistema de fondo, con el propósito de que el terminal móvil pueda utilizarse a continuación en el sistema de telefonía móvil, por ejemplo, para hablar por teléfono, intercambiar datos y otras aplicaciones habituales para terminales móviles. A continuación, por ejemplo, a través de la conexión de intercambio de datos, se realiza una segunda etapa de verificación según el perfeccionamiento de la invención. Solo en el caso de que en la segunda etapa de verificación se haya verificado satisfactoriamente el número de serie y/o el dato de clave-número de serie, el aparato de telefonía móvil se registra en el sistema de fondo. De este modo, en el ciclo de vida del terminal móvil está incorporada una protección adicional, mediante la que se garantiza que solo terminales móviles con un chip original (y dado el caso un sistema operativo de seguridad original) puedan participar en el sistema de telefonía móvil.

A continuación, se explicará más detalladamente la invención por medio de ejemplos de realización y haciendo referencia a los dibujos, en los que muestran:

la figura 1 un sistema para la ilustración de una primera forma de realización de la invención, que comprende un primer perfeccionamiento;

la figura 2 un sistema para la ilustración de una segunda forma de realización de la invención, que comprende el primer perfeccionamiento;

la figura 3 un sistema para la ilustración de un segundo perfeccionamiento de la invención.

La figura 1 muestra un sistema para la ilustración de una primera forma de realización de la invención, en la que la programación de un chip SoC para un terminal de telefonía móvil está protegida por medio de un número de serie SENR, que está formado según una regla de asignación secreta F. El propósito de la programación es, en un chip SoC (*System on chip*) fabricado por un fabricante de chips SOCP (*SOC Provider*), permitir programar un sistema operativo de seguridad por parte de un fabricante de terminales de telefonía móvil OEM (*Original Equipment Manufacturer*). A este respecto, debe garantizarse que solo chips originales del fabricante de chips SOCP se dotan de un sistema operativo de seguridad funcional. El sistema operativo de seguridad comprende una clave de autenticación Kauth, sin la que el sistema operativo de seguridad no es funcional. El fabricante de chips SOCP programa en el chip SoC el número de serie SENR formado según la regla de asignación secreta F y en un módulo de seguridad HSM (*High Security Module*) la regla de asignación secreta F. El fabricante de chips SOCP suministra el chip SoC y el módulo de seguridad HSM al fabricante de terminales OEM. Por regla general, el fabricante de chips SOCP suministra un gran número de chips SoC preparados de esta manera al fabricante de terminales OEM. El fabricante de terminales OEM integra el módulo de seguridad HSM de la manera prevista en su cadena de producción para la programación del chip. De este modo, cada operación de programación para la programación del chip SoC está controlada por el módulo de seguridad HSM, posibilitando así que se haga exclusivamente bajo el control del módulo de seguridad HSM. En primer lugar, el fabricante de terminales OEM programa el sistema operativo de seguridad con la excepción de la clave de autenticación Kauth en el chip SoC. La clave de autenticación Kauth todavía no existe en este momento. En cuanto en el fabricante de terminales OEM se confiere una orden de programación para programar la clave de autenticación Kauth en el chip SoC, el módulo de seguridad HSM lee el número de serie SENR del chip SoC, forma de nuevo el número de serie SENR por medio del número de serie leído SENR y la regla de asignación secreta F almacenada en el módulo de seguridad HSM y compara el número de serie leído y el formado de nuevo SENR. Solo en el caso de que el SENR leído y el formado de nuevo coincidan, se considera el número de serie como verificado en el módulo de seguridad HSM y, directamente en respuesta a la verificación, se genera en el módulo de seguridad HSM la clave de autenticación Kauth. La clave de autenticación Kauth se genera mediante un cálculo criptográfico a partir del número de serie SENR y datos de entrada adicionales, de modo que por tanto la clave de autenticación Kauth es única y específica para el chip SoC, al igual que el número de serie SENR. La clave de autenticación generada Kauth se programa en el chip SoC, sin posibilidad de intervención desde fuera del módulo de seguridad HSM. De este modo se activa el sistema operativo de seguridad. Por el contrario, en el caso de que los números de serie sean diferentes, se emite un aviso de error y/o se interrumpe la programación de chip, opcionalmente también se toma una medida de gestión de errores, tal como, por ejemplo, el borrado de memorias del chip SoC. Es decir, en este caso no se activa el sistema operativo de seguridad.

La figura 2 muestra un sistema para la ilustración de una segunda forma de realización de la invención, en la que la programación de un chip SoC para un terminal de telefonía móvil está protegida por medio de un número de serie SENR y una forma SIG a través del número de serie SENR. Las condiciones de contorno de la programación de chip son tal como se describen en la figura 1. A diferencia de la forma de realización de la figura 1, el fabricante de chips SoCP programa en el chip SoC, en la forma de realización de la figura 2, el número de serie SENR y una firma SIG generada mediante la encriptación del número de serie SENR con una clave criptográfica secreta K. Además, el fabricante de chips SOCP programa la clave criptográfica secreta K en el módulo de seguridad HSM. En cuanto se confiere una orden de programación para programar la clave de autenticación Kauth en el chip SoC, el módulo de seguridad HSM lee del chip SoC la firma SIG y el número de serie SENR, forma de nuevo la firma SIG por medio del número de serie leído SENR y de la clave secreta K almacenada en el módulo de seguridad HSM y compara la

forma leída y la formada de nuevo SIG. En el caso de que las firmas sean diferentes se emite un aviso de error y/o se interrumpe la programación de chip, opcionalmente también se toma una medida de gestión de errores, tal como, por ejemplo, el borrado de memorias del chip SoC. En el caso de que la firma almacenada y la formada de nuevo SIG coincidan, se considera el número de serie SENR como verificado. En respuesta a la verificación, tal como se describe en la figura 1, se forma (calcula) la clave de autenticación Kauth y se programa en el chip SoC, y por consiguiente se activa el sistema operativo de seguridad.

La figura 3 muestra un sistema para la representación de perfeccionamientos de la invención, con la etapa adicional del registro de un terminal móvil que contiene el chip SoC en un sistema de fondo BS de un sistema de telefonía móvil. Hasta la verificación del número de serie SENR en el módulo de seguridad HSM y dado el caso la generación de la clave de autenticación Kauth y el almacenamiento de la misma en el módulo de seguridad HSM, el desarrollo del procedimiento es el mismo que el descrito por medio de la figura 1 o la figura 2. Adicionalmente, después de que en el módulo de seguridad HSM se haya generado la clave de autenticación Kauth y se haya programado en el chip SoC, se genera un dato de clave-número de serie SSD = G(F, Kauth, SENR) o SSD = G(K, Kauth, SENR) por medio de un algoritmo G y usando la información secreta (algoritmo F o clave K) y el número de serie SENR. El dato de clave-número de serie SSD, el número de serie SENR y la información secreta, F o K, representan un conjunto de datos de verificación para una verificación posterior del número de serie del chip SoC. El conjunto de datos de verificación se envía a través de una conexión de datos protegida, en la que no puede influir el fabricante de terminales OEM, a un sistema de fondo BS de un sistema de telefonía móvil. Posteriormente, después de que el terminal móvil, en el que está contenido el chip SoC, se haya vendido a un cliente final, el terminal móvil, para ser funcional en el sistema de telefonía móvil, tiene que registrarse en primer lugar en el sistema de fondo BS. Con motivo del intento de registrar el terminal móvil en el sistema de fondo BS, por medio del dato de clave-número de serie SSD se verifica una vez más el número de serie SENR del chip SoC. Solo en el caso de que el número de serie SENR se verifique satisfactoriamente, el terminal móvil se registra en el sistema de fondo BS y de este modo se posibilita la participación en el sistema de telefonía móvil con el terminal móvil.

REIVINDICACIONES

1. Procedimiento para la programación de un chip (SoC) para un terminal móvil,

- programándose en una etapa preparatoria un número de serie (SENR) en el chip (SoC) y

- verificándose a continuación en una etapa de programación el número de serie (SENR) y realizándose una programación de al menos un dato adicional (Kauth) en el chip (SoC) solo en el caso de que el número de serie (SENR) se haya verificado satisfactoriamente,

verificándose el número de serie (SENR) por medio de un módulo de seguridad (HSM), usando una información secreta (F, K) almacenada en el módulo de seguridad (HSM), que es diferente del número de serie (SENR), y como dato adicional estando prevista una clave criptográfica (Kauth) necesaria para una funcionalidad de un sistema operativo de seguridad implementado o que debe implementarse todavía en el chip (SoC).

2. Procedimiento, según la reivindicación 1, verificándose el número de serie (SENR), al reproducir, usando la información secreta (F, K), el número de serie (SENR) o una información (SIG) dependiente del número de serie (SENR).

3. Procedimiento, según la reivindicación 1 o 2, formándose el número de serie (SENR) mediante una regla de asignación secreta (F), estando almacenada la regla de asignación (F) como información secreta en el módulo de seguridad (HSM).

4. Procedimiento, según la reivindicación 1 o 2, almacenándose en el chip (SoC), además del número de serie (SENR), una firma digital (SIG) formada usando el número de serie (SENR) y una clave secreta (K), estando almacenada la clave secreta (K) como información secreta en el módulo de seguridad (HSM).

5. Procedimiento, según una de las reivindicaciones 1 a 4, estando almacenada en el módulo de seguridad (HSM) la información secreta (F, K) protegida frente a la lectura.

6. Procedimiento, según una de las reivindicaciones 1 a 5, estando previsto como dato adicional un sistema operativo de seguridad o al menos una parte de un sistema operativo de seguridad.

7. Procedimiento, según la reivindicación 6, generándose la clave criptográfica (Kauth) en el módulo de seguridad (HSM).

8. Procedimiento, según la reivindicación 6 o 7, generándose la clave criptográfica (Kauth) usando el número de serie (SENR).

9. Procedimiento para la activación de un sistema operativo de seguridad mediante un procedimiento para la programación según una de las reivindicaciones 6 a 8,

- programándose adicionalmente el sistema operativo de seguridad con la excepción de la clave criptográfica (Kauth) en el chip (SoC) e implementándose de este modo y

- realizándose en la etapa de programación la programación de la clave criptográfica (Kauth) en el chip (SoC) solo en el caso de que el número de serie (SENR) se haya verificado satisfactoriamente.

10. Procedimiento, según una de las reivindicaciones 1 a 9, realizándose la etapa preparatoria por parte de un primer programador (SoCP) y realizándose la etapa de programación por parte de un segundo programador (OEM) separado lógica y/o espacialmente del primer programador (SoCP).

11. Procedimiento, según la reivindicación 10, programándose la información secreta (F, K) por parte del primer programador (SoCP) en el módulo de seguridad (HSM), y proporcionándose el módulo de seguridad (HSM) al segundo programador (OEM) para la etapa de programación.

12. Procedimiento, según una de las reivindicaciones 1 a 11,

- generándose en la etapa de programación en el módulo de seguridad (HSM) un conjunto de datos de verificación que comprende al menos la información secreta (F, K), por medio del que puede verificarse el número de serie (SENR), y enviándose el conjunto de datos de verificación a un sistema de fondo (BS), y

- verificándose una vez más en una etapa de verificación que se encuentra, temporalmente, después de la etapa de programación por medio del conjunto de datos de verificación el número de serie (SENR) en el sistema de fondo (BS), aceptándose el chip (SoC) en el caso de que el número de serie (SENR) se haya verificado satisfactoriamente en la etapa de verificación y rechazándose el chip (SoC) en el caso de que el número de serie (SENR) no se haya

verificado satisfactoriamente en la etapa de verificación.

13. Procedimiento, según la reivindicación 12,

- generándose en la etapa de programación, como al menos una parte del conjunto de datos de verificación, un dato de clave-número de serie dependiente de la clave (Kauth) y del número de serie (SENR) y enviándose al sistema de fondo (BS), y

- verificándose en la etapa de verificación por medio del conjunto de datos de verificación, además del número de serie (SENR) o en lugar del número de serie (SENR), el dato de clave-número de serie.

14. Procedimiento para la configuración asegurada de un terminal móvil que contiene un chip (SoC) para un sistema de telefonía móvil,

- realizándose en el chip (SoC) una etapa preparatoria y una etapa de programación según una de las reivindicaciones 1 a 13,

- llevándose el chip (SoC) con un sistema de fondo (BS) del sistema de telefonía móvil a una conexión de intercambio de datos, para registrar el terminal móvil en el sistema de fondo,

- realizándose una etapa de verificación según la reivindicación 12 o 13, y

- solo en el caso de que en la etapa de verificación se haya verificado satisfactoriamente el número de serie (SENR) y/o el dato de clave-número de serie, registrándose el aparato de telefonía móvil en el sistema de fondo (BS).

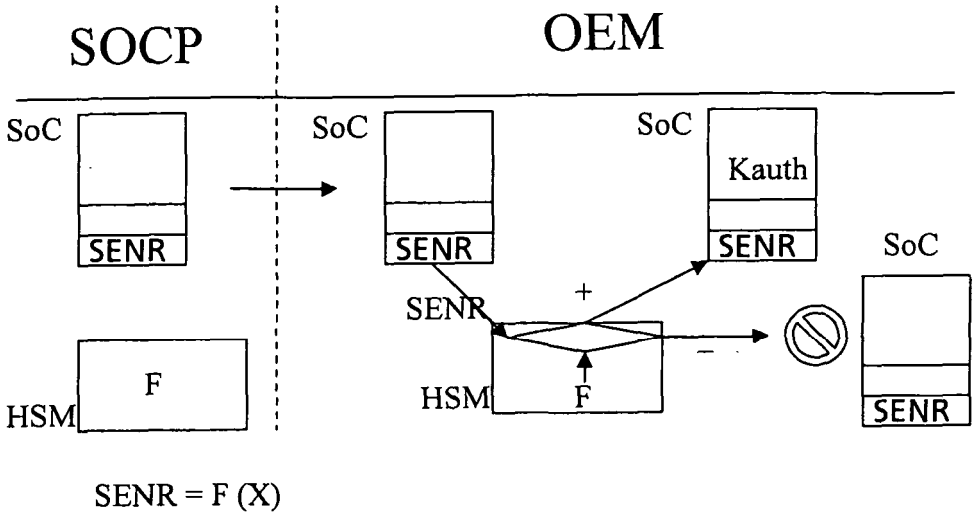

Fig. 1

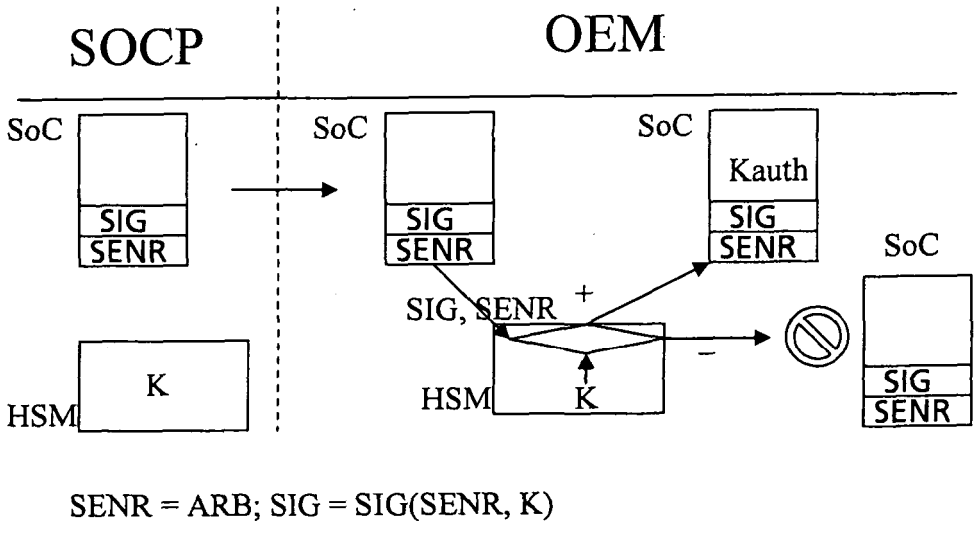

Fig. 2

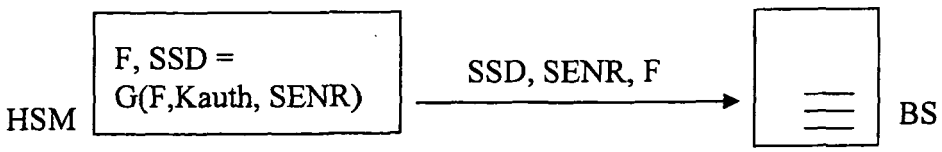

Fig. 3