(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 526 077**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04W 12/06 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.12.2011 E 11815514 (2)**

(97) Fecha y número de publicación de la concesión europea: **24.09.2014 EP 2659616**

(54) Título: **Procedimiento de autentificación de una primera y de una segunda entidades ante una tercera entidad**

(30) Prioridad:

30.12.2010 FR 1061367

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.01.2015

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

MICHAU, BENOÎT y
ROBSHAW, MATTHEW

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de autentificación de una primera y de una segunda entidades ante una tercera entidad

La invención se refiere a un procedimiento de autentificación de al menos dos entidades ante una tercera entidad.

Más precisamente la invención permite autentificar varias entidades que comunican ante una entidad central a través de un canal de comunicación reducido en términos de ancho de banda y de número de mensajes intercambiados.

La invención encuentra una aplicación particularmente interesante en el campo de las telecomunicaciones móviles. Especialmente en el caso en que un operador desea autentificar un dispositivo de tipo tarjeta “SIM”, o tarjeta “USIM” (del inglés “(Universal) Subscriber Identity Module”), así como un terminal que aloja esta tarjeta. Tal autentificación permite asegurarse de que la tarjeta y el terminal están asociados y solo se utilizan juntos. Este caso de figura es cuanto más interesante ya que se desarrollan cada vez más equipos para utilizar la red móvil sin la presencia de un usuario físico que vigile la seguridad de este equipo. Este es el caso por ejemplo de equipos de red tales como retransmisores “LTE” (del inglés “Long term Evolución”) destinados a extender la red de radio al tiempo que tiene un funcionamiento similar a un terminal móvil, o de equipos “M2M” (por «Machine To Machine”) utilizados por ejemplo para aplicaciones de mantenimiento a distancia o de telealarma.

Por ejemplo, una aplicación M2M instalada en un equipo M2M utiliza una red móvil de operador para permitir que un servidor central intercambie informaciones a distancia con este equipo, para obtener informaciones almacenadas en este equipo o modificar el estado sin intervención humana y sobre todo sin vigilancia humana continua del equipo M2M. Para realizar estos intercambios de informaciones a través de la red móvil, el equipo está provisto de una tarjeta de tipo tarjeta USIM. Los equipos M2M, con el mismo título que un terminal móvil de abonado, están sometidos a una autentificación de la red. Más concretamente, hay autentificación de la tarjeta USIM por la red según algoritmos de autentificación conocidos. Sin embargo, en los procedimientos de autentificación de red actuales, el equipo móvil asociado a la tarjeta USIM no es autentificado, ni por la red, ni por la tarjeta USIM. No se puede considerar entonces como un equipo de confianza por la infraestructura de red móvil.

Se han realizado propuestas para solucionar este problema. Por ejemplo, el documento 3GPP http://www.3gpp.org/ftp/tsg sa/WG3 Security/TSGS3 61 Sorrento/DOcs/S3-101404.zip propone un esquema de autentificación de una tarjeta USIM en asociación con un terminal móvil en el que la tarjeta USIM está insertada. Según este esquema, la red y la tarjeta USIM comparten de manera clásica una clave de autentificación K y la red y el terminal comparten una clave simétrica $K_{terminal}$. La autentificación se desarrolla entonces según las siguientes etapas:

- la red envía de manera clásica un reto RAND a la tarjeta USIM,

- la tarjeta USIM calcula una respuesta aplicando un algoritmo F2 de autentificación conocido al reto RAND parametrizado por la clave K; transmite la respuesta al terminal,

- el terminal calcula una firma de esta respuesta mediante la clave simétrica propia del terminal $K_{terminal}$ para producir una nueva respuesta al reto RAND,

- la nueva respuesta es enviada a la red,

- la red puede entonces autentificar el terminal y la tarjeta USIM verificando la firma de la respuesta recibida, y la respuesta como tal.

Sin embargo, esta solución no permite, durante un fallo de la autentificación por la red, identificar si el error de autentificación proviene de la tarjeta USIM, del terminal, o de ambos.

La invención mejora la situación proponiendo un procedimiento de autentificación de una primera entidad y de una segunda entidad por una tercera entidad, compartiendo dichas primera y tercera entidades una primera clave secreta, compartiendo dichas segunda y tercera entidades una segunda clave secreta, comprendiendo el procedimiento etapas:

- de envío por la tercera entidad a la primera entidad de un reto,

- de cálculo por la primera entidad mediante la primera clave secreta de un valor de autentificación en función del reto recibido,

- de envío por la primera entidad a la segunda entidad del valor de autentificación calculado,

- de cálculo por la segunda entidad mediante un algoritmo de cifrado parametrizado por la segunda clave secreta de

una respuesta de autentificación, en función de una ficha conocida de la tercera entidad y de la segunda entidad y del valor de autentificación recibido de la primera entidad,

- de envío por la segunda entidad a la tercera entidad de la respuesta de autentificación,

- de cálculo por la tercera entidad mediante la primera y de la segunda claves secretas de una respuesta de autentificación esperada, en función de la ficha y del reto,

- de comparación de la respuesta de autentificación recibida con la respuesta de autentificación esperada calculada.

De este modo, el procedimiento según la invención permite autentificar dos entidades diferentes que comunican durante una misma autentificación. Las dos entidades autentificadas están de este modo asociadas en el sentido en que su autentificación es realizada conjuntamente por la tercera entidad.

De este modo, esta autentificación permite asegurar que las entidades autentificadas funcionan juntas. Por ejemplo, en el caso de una autentificación de dos entidades en una red móvil en que la primera entidad es una tarjeta SIM, o una tarjeta USIM, y la segunda entidad un terminal en el que la tarjeta (U)SIM está insertada, la autentificación permite asegurar que la tarjeta (U)SIM está bien insertada en el terminal móvil y solo funciona con el terminal. Este aspecto es interesante en términos de seguridad en el caso de equipos M2M o de retransmisores LTE que permanecen sin vigilancia humana.

Por otra parte, gracias al procedimiento de la invención, es posible reutilizar canales e interfaces de comunicación en el inicio definidos para la autentificación de una sola entidad. De este modo, no es necesario modificar interfaces y definir nuevos mensajes entre la tercera entidad encargada de la autentificación y las dos entidades autentificadas. Este aspecto es interesante por ejemplo en el caso de una autentificación de dos entidades en una red móvil. En efecto, hacer evolucionar una interface de la red puede ser un trabajo de larga duración. De una manera general, el procedimiento minimiza los mensajes intercambiados entre la tercera entidad encargada de la autentificación y las dos entidades a autentificar, ya que el número de mensajes intercambiados entre la tercera entidad y las dos entidades es idéntico al número de mensajes intercambiados durante la autentificación de una sola entidad.

Por otra parte, gracias a la invención, es posible durante el fallo de la autentificación de una de las dos entidades identificar cuál de las dos ha fallado. Este aspecto se vuelve posible, por una parte, por la utilización de un algoritmo de cifrado durante la autentificación y, por otra parte, por la compartición de claves secretas respectivas entre una entidad a autentificar y la tercera entidad y de una ficha conocida de las segunda y tercera entidades.

La invención se refiere también a un procedimiento para autentificar una primera y una segunda entidad por una tercera entidad, compartiendo dichas primera y tercera entidades una primera clave secreta, compartiendo dichas segunda y tercera entidades una segunda clave secreta, comprendiendo el procedimiento etapas:

- de envío a la primera entidad de un reto,

- de cálculo mediante la primera y la segunda clave secreta de una respuesta de autentificación esperada, en función de una ficha conocida de la tercera entidad y de la segunda entidad y del reto,

- de recepción procedente de la segunda entidad de una respuesta de autentificación a dicho reto,

- de comparación de la respuesta de autentificación recibida con la respuesta de autentificación calculada.

La invención se refiere asimismo a un procedimiento de autentificación de un grupo constituido por al menos dos entidades ante una tercera entidad, compartiendo la tercera entidad y una primera entidad del grupo una primera clave secreta, compartiendo la tercera entidad y una segunda entidad del grupo una segunda clave secreta, comprendiendo dicho procedimiento las etapas:

- de recepción procedente de la tercera entidad de un reto,

- de cálculo por la primera entidad del grupo mediante la primera clave secreta de un valor de autentificación en función del reto recibido,

- de envío por la primera entidad a la segunda entidad del grupo del valor de autentificación calculado,

- de cálculo por la segunda entidad del grupo mediante un algoritmo de cifrado parametrizado por la segunda clave secreta de una respuesta de autentificación, en función de una ficha conocida de la tercera entidad y de la segunda entidad y del valor de autentificación recibido de la primera entidad,

- de envío por la segunda entidad del grupo a la tercera entidad de la respuesta de autentificación calculada.

En un ejemplo de realización, si la respuesta de autentificación recibida no es igual a la respuesta calculada, el procedimiento comprende también las siguientes etapas, aplicadas por la tercera entidad:

- un descifrado de la respuesta de autentificación recibida mediante la segunda clave secreta,

- una verificación de que la respuesta descifrada comprende la ficha.

Si la verificación es positiva, el procedimiento comprende igualmente un cálculo de un valor esperado a partir del reto y de la primera clave secreta, y una verificación de que la respuesta descifrada comprende el valor esperado.

De este modo, el procedimiento permite, durante el fallo de la autentificación identificar precisamente la entidad que ha fallado. De este modo, es posible, en caso de fallo de la autentificación, imputar el error de autentificación a la segunda entidad o, si la segunda entidad se ha autentificado correctamente ante la primera entidad.

En un ejemplo de realización, la ficha comprende una pluralidad de bits de relleno.

En otro ejemplo de realización, la ficha comprende una parte del reto.

En este modo de realización de la invención, la seguridad del procedimiento de autentificación es mayor ya que la ficha varía de una autentificación a otra.

La invención se refiere asimismo a un dispositivo de autentificación adaptado para autentificar una primera y una segunda entidad, compartiendo dicho dispositivo con la primera entidad una primera clave secreta, y con la segunda entidad una segunda clave secreta, comprendiendo dicho dispositivo:

- medios de envío, dispuestos para enviar un reto a la primera entidad,

- medios de cálculo, dispuestos para calcular una respuesta de autentificación esperada mediante la segunda clave secreta, en función de una ficha conocida del dispositivo de autentificación y de la segunda entidad y de una firma del reto mediante la primera clave secreta,

- medios de recepción, dispuestos para recibir procedente de la segunda entidad una respuesta a dicho reto,

- medios de comparación, dispuestos para comparar la respuesta recibida con la respuesta de autentificación calculada.

La invención se refiere asimismo a un conjunto de dos entidades que comprende una primera y una segunda entidad, adaptándose dicho conjunto para ser autentificado por un dispositivo de autentificación según la invención, compartiendo el dispositivo de autentificación con la primera entidad una primera clave secreta y con la segunda entidad una segunda clave, comprendiendo dicho conjunto:

- medios de recepción, dispuestos para recibir procedente del dispositivo de autentificación un reto,

- primeros medios de cálculo, dispuestos para que la primera entidad del grupo calcule mediante la primera clave secreta un valor de autentificación en función del reto,

- medios de transmisión, dispuestos para que la primera entidad transmita a la segunda entidad del grupo el valor de autentificación,

- segundos medios de cálculo, dispuestos para que la segunda entidad calcule, mediante un algoritmo de cifrado parametrizado por la segunda clave secreta, una respuesta de autentificación, en función de una ficha conocida del dispositivo de autentificación y de la segunda entidad y del valor de autentificación recibido de la primera entidad del conjunto,

- medios de envío, dispuestos para enviar al dispositivo de autentificación la respuesta de autentificación calculada.

La invención se refiere asimismo a un sistema de autentificación que comprende:

- un dispositivo de autentificación según la invención, y

- un conjunto de dos entidades según la invención.

La invención se refiere asimismo a un programa de ordenador en un soporte de datos y cargable en la memoria interna de un dispositivo de autentificación, comprendiendo el programa porciones de código para la ejecución de las etapas del procedimiento de autentificación, que son ejecutadas por el dispositivo cuando el programa es ejecutado en dicho dispositivo.

La invención se refiere asimismo a un soporte de datos en el que se graba el programa de ordenador según la invención.

Numerosos detalles y ventajas de la invención se comprenderán mejor tras la descripción de un modo particular de realización con referencia a los esquemas anexos dados a título no limitativo y en los que:

- la figura 1 describe las etapas del procedimiento de autentificación de dos entidades ante una tercera entidad, según un primer modo particular de realización de la invención;

- la figura 2 representa un ejemplo particular de un dispositivo de autentificación capaz de aplicar el procedimiento de la figura 1;

- la figura 3 representa un ejemplo particular de un grupo de dos entidades capaz de aplicar el procedimiento de la figura 1.

A continuación se describirá el procedimiento de autentificación de dos entidades ante una tercera entidad con relación a la figura 1.

Una primera entidad 10 y una segunda entidad 20 son capaces de ser autentificadas por una tercera entidad 30 durante una misma autentificación. En un ejemplo de realización descrito en este documento, la tercera entidad 30 representa una red de comunicación móvil, tal como la red «GSM» (por “Global System for Mobile Communications”), o la red «GPRS» (del inglés «General Packet Radio Service»). En este caso, la tercera entidad 30 es por ejemplo un centro de autentificación de la red. La primera entidad 10 es por ejemplo una tarjeta de identidad de abonado de tipo tarjeta «SIM» o tarjeta «USIM» (del inglés “(Universal) Subscriber Identity Module”), y la segunda entidad 20 es por ejemplo un terminal móvil en el que la tarjeta de abonado está insertada.

En una fase inicial de configuración P0, se define un cierto número de parámetros destinados a ser utilizados a continuación durante autentificaciones de las primera y segunda entidades 10, 20 ante la tercera entidad 30. La fase de configuración P0 solo se ejecuta una vez. Durante esta fase de configuración P0, se comparte una primera clave secreta K_1 entre la primera entidad 10 y la tercera entidad 30. Se comparte asimismo una segunda clave secreta K_2 entre la segunda entidad 20 y la tercera entidad 30. Por otra parte, durante esta fase inicial de configuración P0, se comparte el conocimiento de una ficha denominada "token" entre la segunda entidad 20 y la tercera entidad 30. La ficha token es un dato numérico, que puede ser fijo o variable. La ficha token es un dato que la segunda entidad 20 y la tercera entidad 30 saben obtener. Por ejemplo, la ficha corresponde a una pluralidad de bits de relleno '0x00'.

Una vez ejecutada la fase de configuración P0, se puede realizar una siguiente fase de autentificación P1. La fase de autentificación P1 se ejecuta tantas veces como sea necesario para que la tercera entidad 30 autentifique conjuntamente las primera y segunda entidades 10, 20. Las siguientes etapas E0 a E10 describen la fase de autentificación P1.

En una etapa inicial E0 de envío de una petición de autentificación, la tercera entidad 30 envía un mensaje de petición de autentificación req_auth a la primera entidad 10. El mensaje de petición de autentificación comprende un reto Chal. El reto Chal es un valor aleatorio elegido por la tercera entidad 30 para la fase de autentificación P1 actual. El mensaje de petición, y por lo tanto el reto Chal, es recibido por la primera entidad 10 durante una etapa E1 de recepción del reto.

En una etapa E2 de cálculo de un valor de autentificación, la primera entidad 10 calcula un valor de autentificación Res_1, en función del reto Chal y de la clave secreta K_1 compartida con la tercera entidad 30. Por ejemplo, la primera entidad 10 calcula el valor de autentificación aplicando un algoritmo de firma al reto Chal, parametrizado por la primera clave secreta compartida K_1. Dicho de otro modo, $Res_1 = Sign(K_1, Chal)$;donde Sign es un algoritmo de firma conocido, por ejemplo un algoritmo “MAC” (del inglés “Mensaje Authenticación Code”). En el caso de las redes GSM, se utiliza el algoritmo A3. En una etapa de envío E3, el valor de autentificación Res_1 es transmitido por la primera entidad 10 a la segunda entidad 20.

En una etapa de recepción E4, la segunda entidad 20 recibe el valor de autentificación Res_1 de la primera entidad 10.

En una etapa E5 de cálculo de una respuesta de autentificación, la segunda entidad 20 calcula una respuesta de autentificación Res_2. Con este fin, la segunda entidad 20 aplica un algoritmo de cifrado Enc, parametrizado por la segunda clave secreta compartida K_2, al valor de autentificación Res_1 recibido de la primera entidad 10 y concatenado con la ficha token. La ficha token es conocida por la tercera entidad 30 y por la segunda entidad 20. Dicho de otro modo, $Res_2 = Enc(K_2, Res_1 \text{ II token})$; donde Enc es un algoritmo de cifrado conocido. Por ejemplo, el algoritmo de cifrado Enc es el algoritmo “AES” (por “Advanced Encrypción Standard”), o el algoritmo “DES” (por “Data Encryption Standard”). Res_2 constituye una respuesta al mensaje de petición de autentificación req_auth enviado por la tercera entidad 30 durante la etapa inicial E0.

En una etapa E6 de envío de la respuesta, la segunda entidad 20 envía a la tercera entidad 30 un mensaje de respuesta resp_auth que comprende la respuesta de autentificación Res_2 calculada durante la etapa E5.

En una etapa de recepción E7, la tercera entidad 30 recibe de la segunda entidad 20 el mensaje de respuesta resp_auth y por lo tanto la respuesta de autentificación Res_2 calculada.

En una etapa E8 de cálculo de una respuesta esperada, la tercera entidad 30 calcula una respuesta de autentificación esperada Res. Con este fin, en una subetapa E8-1 de la etapa E8, la tercera entidad 30 calcula un valor intermediario val_int utilizando la misma función de firma que la aplicada por la primera entidad 10 durante la etapa E2 de cálculo de un valor de autentificación. Dicho de otro modo, la tercera entidad 30 calcula val_int=Sign(K_1, Chal) aplicando el algoritmo de firma Sign, parametrizado por la primera clave compartida K_1, al reto Chal. En una siguiente subetapa E8-2, la tercera entidad 30 calcula la respuesta de autentificación esperada Res aplicando el mismo algoritmo de cifrado que el utilizado por la segunda entidad 20 durante la etapa E5 de cálculo de un resultado de autentificación. Dicho de otro modo, la tercera entidad 30 calcula Res = Enc(K_2, val_int II token) aplicando el algoritmo de cifrado Enc parametrizado por la segunda clave secreta compartida K_2 al valor intermedio val_int obtenido durante la subetapa anterior concatenada con la ficha token.

Se entiende que la etapa E8 de cálculo de un resultado esperado puede ejecutarse independientemente de las etapas ejecutadas por las primera y segunda entidades 10, 20. De este modo, en otro ejemplo de realización del procedimiento, la etapa E8 es ejecutada de manera consecutiva a la etapa E0 de envío de un reto.

En una etapa de comparación E9, la tercera entidad 30 compara la respuesta de autentificación esperada Res, calculada durante la etapa E8 con la respuesta de autentificación Res_2 recibida de la segunda entidad 20 durante la etapa E7.

Si la comparación es positiva (rama ok en la figura 1), es decir si la respuesta de autentificación calculada Res es igual a la respuesta de autentificación Res_2 recibida de la segunda entidad 20, entonces la autentificación de las primera y segunda entidades ha tenido éxito. Las dos entidades han sido por lo tanto correctamente autentificadas durante una misma fase de autentificación. La tercera entidad 30 se encuentra entonces en un estado E10 de autentificación conseguida.

Si la comparación es negativa (rama Nok en la figura 1) entonces, se procede a un análisis durante una fase P2 de análisis con el fin de determinar si el error de autentificación procede de la segunda entidad 20, o, si se ha conseguido la autentificación de la segunda entidad 20, de la primera entidad 10.

De este modo, en una etapa E11 de descifrado, la tercera entidad 30 procede al descifrado de la respuesta de autentificación Res_2 recibida de la segunda entidad 20 mediante la segunda clave secreta compartida K_2. Con este fin, la tercera entidad 12 calcula $Enc^{-1}(K_2, Res_2)$, donde Enc^{-1} representa el algoritmo de descifrado asociado al algoritmo de cifrado Enc. Se observa que cuando la autentificación tiene éxito, la respuesta de autentificación descifrada es igual a la concatenación de un primer valor correspondiente a la firma del reto Chal mediante la primera clave secreta compartida K_1, a un segundo valor correspondiente a la ficha token. Dicho de otro modo, en caso de autentificación conseguida, se verifica la siguiente igualdad:

$$Enc^{-1}(K_2, Res_2) = Sign\ (K_1, Chal)\ ||\ token$$

Se observa que al ser conocida por la tercera entidad 30 la dimensión de la ficha token, es fácil para la tercera entidad 30 distinguir el primer y el segundo valor.

En una etapa E12 de verificación de la ficha, se verifica si la ficha token conocida por la segunda y por la tercera entidades 20, 30 es efectivamente igual al segundo valor comprendido en la respuesta de autentificación descifrada. Si la verificación es positiva, entonces la segunda entidad 20 se ha autentificado correctamente. Si la verificación es negativa, es decir si la ficha token no está comprendida en la respuesta de autentificación descifrada, entonces la autentificación de la segunda entidad 20 ha fallado. En efecto, en este caso, o bien la segunda entidad 20 no ha utilizado la ficha token convenida durante la fase de configuración P0, o bien no ha utilizado el algoritmo correcto de cifrado Enc, o bien no ha utilizado la segunda clave secreta compartida K_2. En estos tres casos, la autentificación de la segunda entidad 20 falla.

Si la verificación de la ficha efectuada durante la etapa E12 es positiva (rama ok en la figura), es decir si la autentificación de la segunda entidad 20 tiene éxito, entonces, en una siguiente etapa E13 de verificación de firma, la tercera entidad 30 verifica la primera parte de la respuesta de autentificación descifrada. De este modo, la tercera entidad 30 calcula un valor esperado aplicando el algoritmo de firma Sign al reto Chal parametrizado por la primera clave secreta compartida K_1. Dicho de otro modo, la tercera entidad 30 calcula Sign(K_1, Chal). Si el valor esperado no es igual al primer valor comprendido en la respuesta de autentificación descifrada, entonces la autentificación de la primera entidad 10 ha fallado.

Se observa que durante la fase de análisis P2, es posible imputar un error de autentificación a la segunda entidad 20, o, si la autentificación de la segunda entidad 20 tiene éxito, a la primera entidad 10.

La invención se describe en este punto en el marco de una autentificación por la red GSM o GPRS de una tarjeta (U)SIM en asociación con un terminal móvil en el que la tarjeta está insertada. La invención no se limita evidentemente à estas redes. De este modo el procedimiento se aplica asimismo a una autentificación en otras redes, por ejemplo una red “UMTS” (por “Universal Mobile Telecommunication System”). En este ejemplo, el algoritmo de firma aplicado por la primera entidad 10 para calcular el valor de autentificación es entonces el algoritmo “AKA” (del inglés Authentication Key Agreement”).

Asimismo, el procedimiento no se limita a una autentificación en una red móvil de una tarjeta (U)SIM y de un terminal. Más en general, el procedimiento se aplica a la autentificación por una tercera entidad de dos entidades que comunica. De este modo, en otro ejemplo de realización, se procede a una autentificación conjunta por una red de una tarjeta (U)SIM y de una entidad externa al terminal móvil, por ejemplo un componente “RFID” (por “Radio Frequency Identification”) aplicada en un producto para comprar. En este caso, el terminal, está adaptado para funcionar en modo lector de etiquetas RFID. La tarjeta (U)SIM y la etiqueta son capaces de comunicar a través del terminal móvil. De este modo, la autentificación conjunta de la tarjeta (U)SIM y de la etiqueta RFID puede corresponder a la obtención protegida de un recibido que valida la compra del producto mediante el terminal. En otro caso de uso, la segunda entidad está asociada a un dispositivo externo, por ejemplo un parámetro que integra un componente “NFC” (del inglés “Near Field Communication”). El terminal hace las veces de borna NFC y la autentificación conjunta de la tarjeta (U)SIM y del parámetro como tarjeta NFC por la red valida la compra a través del terminal de un ticket de estacionamiento.

Se precisa que durante la fase de configuración P0 son distribuidas respectivamente claves secretas K_1, K_2 a la primera y la segunda entidades 10, 20, estando cada una de las claves compartida con la tercera entidad 30. En el ejemplo descrito en el presente documento de una red móvil, la primera entidad es una tarjeta (U)SIM y la segunda entidad es un terminal en el que la tarjeta está insertada. La primera clave secreta K_1, habitualmente denominada clave de autentificación se define e instala en la tarjeta (U)SIM durante la etapa de fabricación de la tarjeta. La segunda clave secreta K_2 puede instalarse en el terminal una vez que el equipo se pone en circulación. Esta instalación puede hacerse de manera protegida por ejemplo mediante un sistema de criptografía de claves públicas instalado durante la fabricación del terminal y destinado a permitir la instalación protegida de la segunda clave secreta compartida K_2 desde la tercera entidad, o desde una entidad de distribución de claves dedicada. En este caso, la entidad de distribución de claves distribuye entonces la segunda clave compartida K_2 a las segunda y tercera entidades 20, 30.

La ficha token, conocida de las segunda y tercera entidades 20, 30, puede ser fija. Por ejemplo, como se ha apreciado anteriormente, puede consistir en bits de relleno '0x00' (se habla habitualmente de bits de padding). En otro ejemplo de realización, la ficha token puede ser variable y corresponder a una parte del reto Chal enviado al inicio de la fase de autentificación. En este caso, la tercera entidad 30 y la segunda entidad 20 acuerdan durante la fase de configuración P0 qué parte del reto corresponde a la ficha. Por ejemplo, son los x primeros bits del reto los que constituyen la ficha, los x últimos, los x primeros bits de peso fuerte, etc.

La dimensión de la ficha debe ajustarse de manera que la seguridad de la autentificación y la dimensión máxima autorizada del resultado de autentificación transmitido por la segunda entidad 20 a la tercera entidad 30 sean compatibles. De este modo, en un ejemplo de realización que corresponde a una autentificación en una red móvil de tercera generación, en la que un resultado de autentificación está habitualmente comprendido entre 32 y 128 bits, parece razonable tener fichas de dimensión comprendida entre 32 y 64 bits. De este modo, la respuesta de autentificación tiene una dimensión comprendida entre 64 y 96 bits. Por otra parte, por razones de compatibilidad con la interfaz de radio ofrecida por la red, la respuesta de autentificación Res_1 calculada por la primera entidad 10, aquí la tarjeta (U)SIM, puede truncarse. Por ejemplo, cuando la tarjeta (U)SIM está configurada para producir valores de autentificación Res_1 de 128 bits, y cuando la interfaz de radio con la red está entonces adaptada para transmitir tañes respuestas, parece necesario truncar el valor de autentificación producida por la tarjeta (U)SIM para tener en cuenta la ficha token. En efecto, la ficha token está concatenada con el valor de autentificación Res_1 por la segunda entidad 20, aquí el terminal. De este modo, en este ejemplo, el valor de autentificación Res_1 puede truncarse con 64 o 96 bits por la primera entidad 10, lo cual permite utilizar una ficha de 64 o 32 bits. Evidentemente, en este caso, durante la etapa E8 de cálculo de respuesta esperada, la tercera entidad 30, aquí la red, trunca asimismo el valor intermedio val_int que calcula.

A continuación se describe un ejemplo particular de dispositivo de autentificación 30 capaz de aplicar el procedimiento de la figura 1 en relación con la figura 2. El dispositivo de autentificación 30 es capaz de autentificar un grupo de al menos dos entidades (no representadas en la figura 2). El dispositivo de autentificación 30 es por ejemplo un servidor de autentificación de una red móvil en el caso en que el procedimiento se refiera a la autentificación por la red de dos entidades. En otro ejemplo de realización, el dispositivo de autentificación es un terminal móvil, capaz de autentificar una tarjeta (U)SIM y una entidad exterior al terminal.

En todos estos casos, el dispositivo de autentificación comprende:

- un procesador 301, o "CPU" (del inglés "Central Processing Unit"), o unidad de procesamiento. El procesador 301 está conectado a un conjunto de memorias:

- una memoria viva 302, o "RAM" (por "Random Access Memory), permite efectuar cálculos, cargar instrucciones y ejecutarlas,

- una memoria muerta 303, o memoria no volátil, o "ROM" (por "Read Only Memory"), adaptada para memorizar datos no volátiles, por ejemplo algoritmos criptográficos.

De este modo, la memoria 303 memoriza un algoritmo de firma Sign y un algoritmo de cifrado Enc. Memoriza asimismo una ficha token, o un medio que permite la obtención de esta ficha. La memoria 303 está adaptada asimismo para almacenar en una zona protegida las claves secretas que el dispositivo de autentificación comparte con las entidades a autentificar. Por ejemplo la memoria memoriza una primera clave secreta K_1 compartida con la primera entidad a autentificar, y una segunda clave secreta K_2 compartida con la segunda entidad a autentificar.

El dispositivo de autentificación 30 aloja asimismo una aplicación en forma de un programa, capaz de aplicar las etapas del procedimiento de la invención ejecutadas por el dispositivo. Con este fin, el dispositivo 30 comprende asimismo:

- Medios de envío 304, dispuestos para enviar a la primera entidad a autentificar un mensaje de petición de autentificación que comprende un reto Chal.

- Medios de cálculo 305, dispuestos para calcular una respuesta de autentificación esperada Res. Para ello, en funcionamiento, el dispositivo 30 aplica el algoritmo de cifrado Enc parametrizado por la segunda clave secreta K_2 memorizada a un dato obtenido por concatenación de un primer valor con la ficha token. El primer valor se obtiene aplicando el algoritmo de firma parametrizado por la primera clave secreta compartida K_1 al reto Chal. Los medios de cálculo 305 están adaptados para aplicar la etapa E8 de cálculo de una respuesta esperada del procedimiento de autentificación descrito anteriormente.

- Medios de recepción 306, dispuestos para recibir procedente de la segunda entidad un mensaje de respuesta a la petición de autentificación al reto enviado por los medios de envío 304. Los medios de recepción 306 están adaptados para aplicar la etapa E7 de recepción del procedimiento de autentificación descrito anteriormente.

- Medios de comparación 307, dispuestos para comparar la respuesta de autentificación recibida de la segunda entidad con el resultado de autentificación calculado por les medios de cálculo 305. Los medios de comparación 307 están adaptados para aplicar la etapa E9 de comparación del procedimiento de autentificación descrito anteriormente.

- Medios de análisis 308, dispuestos para identificar de donde procede un error de autentificación detectado por los medios de comparación 307. Los medios de análisis 308 comprenden:

• Medios de descifrado 308-1, dispuestos para descifrar la respuesta de autentificación Res_2 recibida de la segunda entidad mediante la segunda clave secreta compartida K_2. Los medios de descifrado 308-1 están adaptados para aplicar la etapa de descifrado E11 del procedimiento de autentificación.

• Medios 308-2 de verificación de la ficha, dispuestos para verificar que la ficha conocida del dispositivo de autentificación 30 está comprendida en la respuesta de autentificación descifrada por los medios de descifrado 308-1. Los medios 308-2 están adaptados para aplicar la etapa E12 de verificación de la ficha del procedimiento de autentificación descrita anteriormente.

• Medios 308-3 de verificación de firma, dispuestos para verificar que la primera parte de la respuesta de autentificación descifrada es efectivamente conforme a una firma del reto mediante el algoritmo Sign parametrizado por la primera clave secreta K_1. Los medios 308-3 están adaptados para aplicar la etapa E13 de verificación de firma del procedimiento de autentificación descrito anteriormente.

Los medios de envío 304, los medios de cálculo 305, los medios de recepción 306, los medios de comparación 307, los medios de análisis 308 que comprenden los medios de descifrado 308-1, los medios 308-2 de verificación de la ficha y los medios 308-3 de verificación de firma son preferiblemente módulos de software que comprenden instrucciones de software para ejecutar las etapas correspondientes del procedimiento descrito anteriormente por el dispositivo de autentificación 30. Los módulos de software pueden almacenarse en o transmitirse por un soporte de datos. El mismo puede ser un soporte material de almacenamiento, por ejemplo un CD-ROM, una memoria magnética, o bien un soporte de transmisión tal como una señal o una red de telecomunicaciones.

A continuación se describe un ejemplo particular de un conjunto 40 de dos entidades, adaptado para ser

autentificado por un dispositivo de autentificación 30 descrito anteriormente en relación con la figura 3.

Este conjunto 40 comprende una primera entidad y una segunda entidad no representadas en la figura 3.

El conjunto de entidades comprende:

- Una unidad de procesamiento 401, o CPU. Se entiende que cada una de las dos entidades posee una unidad de procesamiento que le es propia. Este conjunto de CPU está representado en la figura 3 por la unidad de procesamiento 401. La unidad de procesamiento está conectada a una pluralidad de memorias:

• Una memoria viva 402, o memoria RAM, adaptada para permitir efectuar cálculos, cargar instrucciones y ejecutarlas. Aquí también, se entiende que cada entidad dispone de una memoria RAM que le es propia. El conjunto de estas memorias RAM está representado por la memoria 402.

• Una memoria no volátil 403, o memoria ROM, adaptada para memorizar datos non volátiles, por ejemplo algoritmos criptográficos. Se entiende que cada entidad dispone de tal memoria. Sin embargo, el conjunto de la memoria de las entidades está representado por una sola memoria ROM 403. La memoria 403 memoriza algoritmos criptográficos, en particular el algoritmo de firma Sign adaptado para calcular el valor de autentificación y el algoritmo de cifrado Enc adaptado para calcular la respuesta de autentificación Res_2. Memoriza asimismo una ficha token, o un medio que permite la obtención de esta ficha. La memoria 403 memoriza asimismo en una zona protegida claves secretas compartidas con el dispositivo de autentificación. En particular, memoriza una primera clave secreta compartida K_1 y una segunda clave secreta compartida K_2.

- Medios de recepción 404, dispuestos para recibir procedente del dispositivo de autentificación un mensaje de petición de autentificación que comprende un reto. Los medios de recepción 404 aplican la etapa E1 de recepción de un reto del procedimiento de autentificación descrito anteriormente.

- Primeros medios de cálculo 405, dispuestos para que la primera entidad del conjunto calcule mediante la primera clave secreta K_1 un valor de autentificación mediante el algoritmo de firma Sign aplicado al reto recibido por los medios de recepción 404. Los primeros medios de cálculo 405 están adaptados para aplicar la etapa E2 de cálculo de un valor de autentificación del procedimiento de la invención.

- Medios de transmisión 406, dispuestos para que la primera entidad transmita a la segunda entidad del conjunto el valor de autentificación calculada por los medios de cálculo 405. Los medios de transmisión 406 están adaptados para aplicar la etapa E3 de envío del valor de autentificación del procedimiento de autentificación.

- Segundos medios de cálculo 407, dispuestos para que la segunda entidad calcule una respuesta de autentificación Res_2, aplicando el algoritmo de cifrado Enc parametrizado por la segunda clave secreta K_2 al valor de autentificación calculado por la primera entidad del conjunto. Los segundos medios de cálculo 407 están adaptados para aplicar la etapa E5 de cálculo de una respuesta de autentificación del procedimiento descrito anteriormente.

- Medios de envío 408, dispuestos para enviar al dispositivo de autentificación un mensaje de respuesta que comprende la respuesta de autentificación calculada por los segundos medios de cálculo 407. Los medios de envío están adaptados para aplicar la etapa E6 de envío de la respuesta de autentificación.

Los medios de recepción 404, los primeros medios de cálculo 405, los medios de transmisión 406, los segundos medios de cálculo 407 y los medios de envío 408 son preferiblemente módulos de software que comprenden instrucciones de software para ejecutar las etapas del procedimiento descrito anteriormente por el conjunto constituido por las dos entidades. Los módulos de software pueden almacenarse en o transmitirse por un soporte de datos. El mismo puede ser un soporte material de almacenamiento, por ejemplo un CD-ROM, una memoria magnética, o bien un soporte de transmisión tal como una señal o una red de telecomunicaciones.

La invención se refiere asimismo a un sistema de autentificación que comprende un dispositivo de autentificación 30 y un conjunto 40 de al menos dos entidades.

REIVINDICACIONES

1. Procedimiento de autentificación de una primera entidad (10) y de una segunda entidad (20) por una tercera entidad (30), compartiendo dichas primera y tercera entidades una primera clave secreta (K_1), compartiendo dichas segunda y tercera entidades una segunda clave secreta (K_2), comprendiendo el procedimiento etapas:

- de envío (E0) por la tercera entidad a la primera entidad de un reto (Chal),

- de cálculo (E2) por la primera entidad mediante la primera clave secreta de un valor de autentificación (Res_1) en función del reto recibido,

- de envío (E3) por la primera entidad a la segunda entidad del valor de autentificación calculada,

- de cálculo (E5) por la segunda entidad mediante un algoritmo de cifrado parametrizado por la segunda clave secreta de una respuesta de autentificación (Res_2), en función de una ficha conocida de la tercera entidad y de la segunda entidad y del valor de autentificación recibida de la primera entidad,

- de envío (E6) por la segunda entidad a la tercera entidad de la respuesta de autentificación,

- de cálculo (E8) por la tercera entidad mediante la primera y la segunda claves secretas de una respuesta de autentificación esperada (Res), en función de la ficha y del reto,

- de comparación (E9) de la respuesta de autentificación recibida con la respuesta de autentificación esperada calculada.

2. Procedimiento para autentificar una primera y una segunda entidad por una tercera entidad, compartiendo dichas primera y tercera entidades una primera clave secreta (K_1), compartiendo dichas segunda y tercera entidades una segunda clave secreta (K_2), comprendiendo el procedimiento etapas:

- de envío (E0) a la primera entidad de un reto (Chal),

- de cálculo (E8) mediante un algoritmo de cifrado, parametrizado por la segunda clave secreta, de una respuesta de autentificación esperada (Res), en función de un ficha conocida de la tercera entidad y de la segunda entidad, y de una firma del reto mediante la primera clave secreta,

- de recepción (E7) procedente de la segunda entidad de una respuesta de autentificación (Res_2) a dicho reto,

- de comparación (E9) de la respuesta de autentificación recibida con la respuesta de autentificación calculada.

3. Procedimiento de autentificación de un grupo constituido por al menos dos entidades (10, 20) ante una tercera entidad (30), compartiendo la tercera entidad y una primera entidad (10) del grupo una primera clave secreta (K_1), compartiendo la tercera entidad y una segunda entidad (20) del grupo una segunda clave secreta (K_2), comprendiendo dicho procedimiento las etapas:

- de recepción (E1) procedente de la tercera entidad de un reto,

- de cálculo (E2) por la primera entidad del grupo mediante la primera clave secreta de un valor de autentificación (Res_1) en función del reto recibido,

- de envío (E3) por la primera entidad a la segunda entidad del grupo del valor de autentificación calculada,

- de cálculo (E5) por la segunda entidad del grupo mediante un algoritmo de cifrado parametrizado por la segunda clave secreta de una respuesta de autentificación (Res_2), en función de una ficha conocida de la tercera entidad y de la segunda entidad y del valor de autentificación recibido de la primera entidad,

- de envío (E6) por la segunda entidad del grupo a la tercera entidad de la respuesta de autentificación calculada.

4. Procedimiento según la reivindicación 1 o la reivindicación 2, que comprende, si la respuesta de autentificación recibida no es igual a la respuesta calculada, etapas aplicadas por la tercera entidad:

- un descifrado (E11) de la respuesta de autentificación recibida mediante la segunda clave secreta (K_2),

- una verificación (E12) que la respuesta descifrada comprende la ficha.

5. Procedimiento según la reivindicación 4, que comprende, si la verificación es positiva:

- un cálculo (E13) de un valor esperado a partir del reto y de la primera clave secreta (K_1), y una verificación de que la respuesta descifrada comprende el valor esperado.

6. Procedimiento según una de las reivindicaciones anteriores, en el que la ficha comprende una pluralidad de bits de relleno.

7. Procedimiento según una de las reivindicaciones 1 a 5, en el que la ficha comprende una parte del reto.

8. Dispositivo de autentificación (30) adaptado para autentificar una primera y una segunda entidad, compartiendo dicho dispositivo con la primera entidad una primera clave secreta (K_1), y con la segunda entidad una segunda clave secreta (K_2), comprendiendo dicho dispositivo:

- medios (304) de envío, dispuestos para enviar un reto (Chal) a la primera entidad,

- medios (305) de cálculo, dispuestos para calcular, mediante un algoritmo de cifrado, parametrizado por la segunda clave secreta, una respuesta de autentificación esperada (Res), en función de un ficha conocida del dispositivo de autentificación y de la segunda entidad, y de una firma del reto mediante la primera clave secreta,

- medios (306) de recepción, dispuestos para recibir procedente de la segunda entidad una respuesta (Res_2) a dicho reto,

- medios (307) de comparación, dispuestos para comparar la respuesta recibida con la respuesta de autentificación calculada.

9. Conjunto de dos entidades que comprende una primera y una segunda entidad, estando dicho conjunto adaptado para ser autentificado por un dispositivo de autentificación según la reivindicación 8, compartiendo el dispositivo de autentificación con la primera entidad una primera clave secreta (K_1) y con la segunda entidad una segunda clave (K_2),comprendiendo dicho conjunto:

- medios (404) de recepción, dispuestos para recibir procedente del dispositivo de autentificación un reto,

- primeros medios (405) de cálculo, dispuestos para que la primera entidad del grupo calcule mediante la primera clave secreta un valor de autentificación (Res_1) en función del reto,

- medios (406) de transmisión, dispuestos para que la primera entidad transmita a la segunda entidad del grupo el valor de autentificación,

- segundos medios (407) de cálculo, dispuestos para que la segunda entidad calcule, mediante un algoritmo de cifrado parametrizado por la segunda clave secreta, una respuesta de autentificación (Res_2), en función de una ficha conocida del dispositivo de autentificación y de la segunda entidad y del valor de autentificación recibido de la primera entidad del conjunto,

- medios (408) de envío, dispuestos para enviar al dispositivo de autentificación la respuesta de autentificación calculada.

10. Sistema de autentificación que comprende

- un dispositivo de autentificación según la reivindicación 8, y

- un conjunto de dos entidades según la reivindicación 9.

11. Programa de ordenador en un soporte de datos y cargable en la memoria interna de un dispositivo de autentificación, comprendiendo el programa porciones de código para la ejecución de las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 7 cuando el programa es ejecutado en dicho dispositivo.

12. Soporte de datos en el que se graba el programa de ordenador según la reivindicación 11.

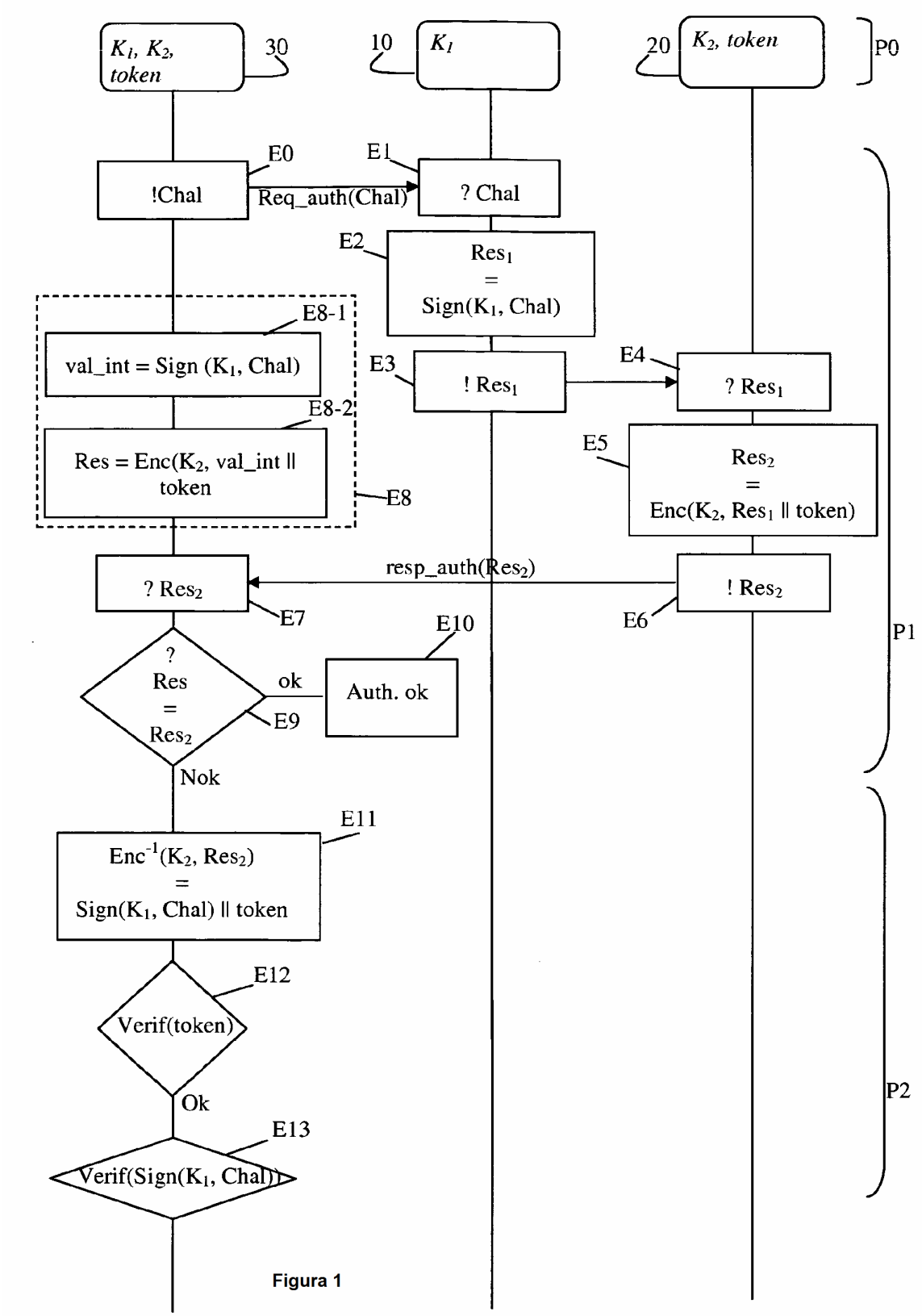
K_1, K_2, token
30
10
K_1
20
K_2, token
P0
E0
E1
!Chal
Req_auth(Chal)
? Chal
E2
Res_1 = $Sign(K_1, Chal)$
E8-1
val_int = Sign (K_1, Chal)
E3
! Res_1
E4
? Res_1
E8-2
Res = $Enc(K_2, val\_int \| token)$
E8
E5
Res_2 = $Enc(K_2, Res_1 \| token)$
resp_auth(Res_2)
? Res_2
! Res_2
E7
E6
E10
P1
?
Res
=
Res_2
ok
Auth. ok
E9
Nok
E11
$Enc^{-1}(K_2, Res_2)$ = $Sign(K_1, Chal) \| token$
E12
Verif(token)
Ok
E13
Verif(Sign(K_1, Chal))
P2

Figura 1

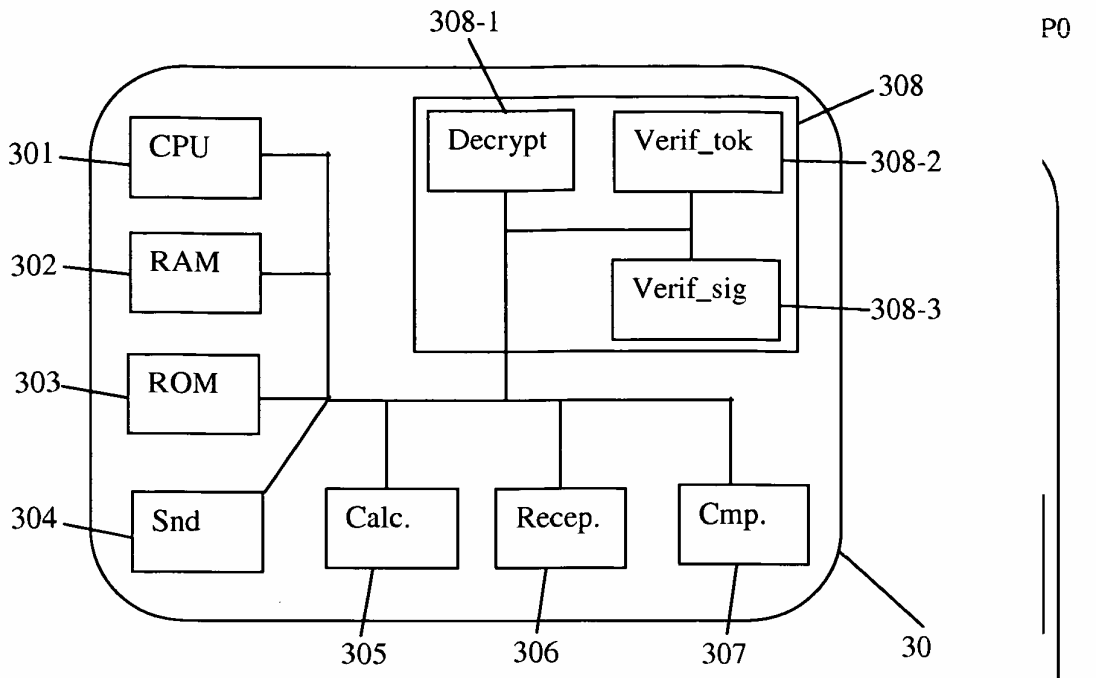

Figura 2

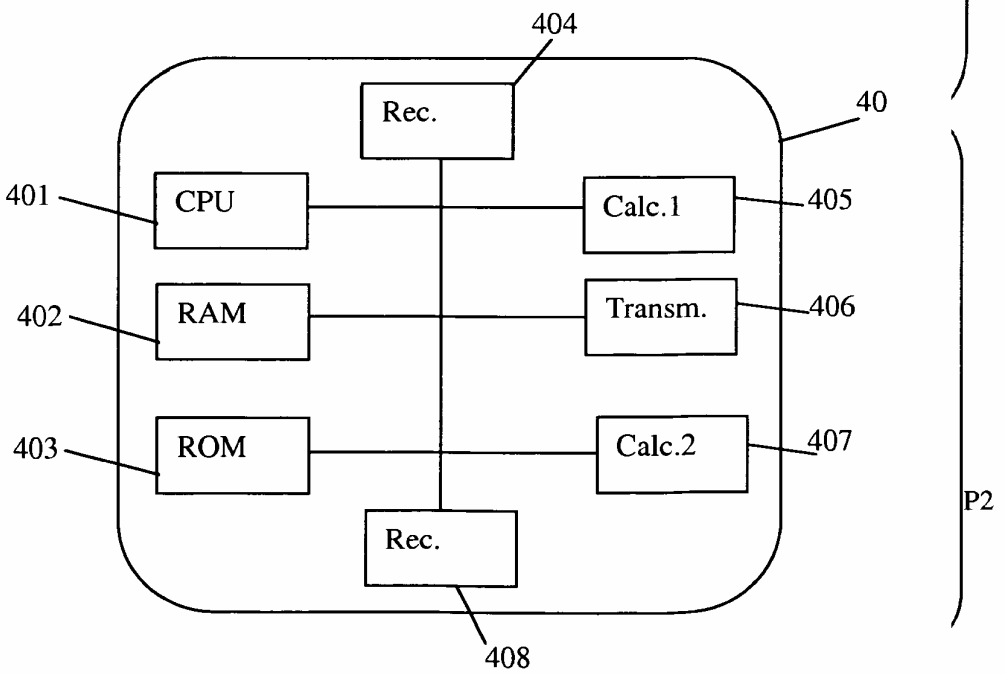

Figura 3