(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 315 677**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04744327 .0**
(96) Fecha de presentación : **30.08.2004**
(97) Número de publicación de la solicitud: **1665726**
(97) Fecha de publicación de la solicitud: **07.06.2006**

(54) Título: **Método de autenticación y tarjeta inteligente para comunicación de datos.**

(30) Prioridad: **09.09.2003 EP 03292219**

(45) Fecha de publicación de la mención BOPI:
01.04.2009

(45) Fecha de la publicación del folleto de la patente:
01.04.2009

(73) Titular/es: **Gemalto S.A.**
6 rue de Verrerie
92190 Meudon, FR

(72) Inventor/es: **Bernard, Eddy y**
Salgado, Stéphanie

(74) Agente: **Elzaburu Márquez, Alberto**

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Método de autentificación y tarjeta inteligente para comunicación de datos.

Antecedentes del invento

Campo del invento

Este invento está relacionado con la autenticación en la comunicación de datos. Se relaciona, en particular, pero sin limitarse a ellas, con estaciones móviles de autenticación y servidores de red que se comunican mediante una red como la Internet.

El ejemplo que ilustrará el invento es el de un sistema de comunicación móvil que comprende una red de comunicación móvil y estaciones móviles. En este ejemplo, la red proporciona un servicio a una estación móvil tras la autenticación de la estación móvil. La estación móvil incluye un módulo portátil como una tarjeta USIM y un equipo móvil (auricular) que puede comunicarse con la red y el módulo portátil.

Antecedentes de la técnica

Las presentes normas de tercera generación (3G) (en particular TS 31.102 y TS 33.102) definen el protocolo de autenticación en una red 3G (conocido como protocolo AKA por sus siglas en inglés, Autenticación y gestión de claves) entre la tarjeta USIM y un Centro de autenticación (AuC).

En este contexto, la tarjeta recibe una solicitud llamada de autenticación compuesta de varios campos de datos:

- un desafío aleatorio (RAND);
- un número de secuencia (SQN) o un número de secuencia oculto (SQN⊕AK)
- un código de autenticación de mensajes (MAC),

Donde:

AK es una clave de anonimato, el símbolo ⊕ es el OR exclusivo bit a bit, MAC es el código de autenticación de mensajes, SQN es un número de secuencia que puede indicar a partir de su valor si la solicitud en curso es una solicitud reiterada o no.

Tras la recepción de estos campos de datos, la tarjeta calcula el SQN (si se requiere), verifica el MAC y comprueba a partir del SQN que no se haya enviado la misma solicitud.

Para calcular el SQN (si se requiere), la USIM:

- calcula la clave de anonimato AK con la función f5 (RAND, K)
- recupera eventualmente el número de secuencia SQN mediante el (SQN ⊕AK) ⊕ AK = SQN

f5 es una función de generación de clave utilizada para calcular AK.

K es una clave secreta a largo plazo que comparten la tarjeta y el servidor.

A continuación, la tarjeta también genera un código de autenticación de mensaje esperado XMAC utilizando el RAND, K, SQN, un campo de gestión adicional (AMF) y una función f1 de autenticación.

Posteriormente, la tarjeta compara el XMAC con el MAC que ha sido incluido en la solicitud de autenticación. Si son diferentes, la tarjeta envía al auricular un mensaje de rechazo de la autenticación indicando el motivo y la tarjeta cancela el proceso de autenticación en curso. En este caso, el AuC puede iniciar un nuevo proceso de identificación y autenticación del cliente.

La tarjeta también verifica que el número de secuencia recibido SQN esté en el rango correcto. El SQN puede no diferir más que una cantidad predeterminada del SQN almacenado en la tarjeta. Si la tarjeta considera que el número de secuencia no está en el rango correcto, envía un mensaje de fallo de sincronización al AuC y cancela el proceso en curso.

Dicho proceso de autenticación se menciona en EP-A-1 156 694. Se pueden obtener más detalles o explicaciones respecto a las etapas anteriores en las normas mencionadas como referencia.

El código MAC (y por lo tanto XMAC) se calcula a partir de todos los datos de la solicitud y la misma clave de autenticación que la de la entidad solicitante. Su función es asegurar que los datos solicitados no hayan sido alterados

durante la transmisión y la tarjeta también garantiza que la entidad solicitante en realidad posee la misma clave de autenticación que la tarjeta.

Mientras la tarjeta verifica la integridad y autenticidad de los datos recibidos desde el servidor, la tarjeta calcula el XMAC con un mecanismo que incluye los datos a ser verificados junto con la clave K de autenticación. En estas circunstancias, un atacante puede forzar la utilización de la clave de autenticación enviando a la tarjeta una solicitud de autenticación con datos seleccionados estratégicamente. Utilizando varios métodos, como ataques por canales laterales y perturbaciones, la información puede ser revelada, lo que origina la obtención total o parcial de la clave de autenticación.

Para que se puedan llevar a cabo, la mayoría de ataques requieren una cantidad determinada de solicitudes de autenticación dependiendo de la fuerza del algoritmo utilizado para calcular el XMAC. En cada uno de estos intentos, el atacante debe proporcionar un MAC falso (debido a que desconoce el valor real de la clave).

En sistemas conocidos como el mencionado en el documento EP-A-1 156 694, en caso de detección de interferencia sospechosa, es decir cuando MAC y XMAC no coinciden, se sugiere enviar a la entidad solicitante un mensaje rogando se retransmita el mensaje, luego verificar si el mensaje recibido es correcto o no, y determinar el procedimiento en un caso negativo. Sin embargo, el sistema mencionado en este documento no ofrece ningún recurso para rastrear dicha sucesión de eventos, de tal manera que no se puede evitar que el atacante, tras la cancelación de un proceso de autenticación dado, repita el mismo proceso o una serie de procesos adicionales, hasta lograr burlar el sistema y acceder a los datos protegidos.

Resumen del invento

El objetivo del invento es limitar el número de ataques consecutivos en una tarjeta USIM, limitando específicamente el número de intentos reiterados de autenticación.

El invento establece un método como el mencionado en EP-A-1 156 694, es decir un método de autenticación para ser utilizado en un sistema que incluye una primera entidad y una segunda entidad comunicadas por medio de una red, donde la primera entidad se adapta para autenticar a la segunda entidad y los datos que recibe de ésta; y donde ambas entidades poseen la misma clave secreta. El método comprende los siguientes pasos u operaciones:

- recepción por parte de dicha primera entidad de un código de autenticación de mensajes y otros parámetros, siendo dicho código de autenticación de mensajes una función de dicha clave secreta y de dichos otros parámetros.

- cálculo por parte de dicha primera entidad de un código esperado a partir de dichos otros parámetros que han sido recibidos y de dicha clave secreta que posee la primera entidad;

- comparación por parte de dicha primera entidad de dicho código de autenticación de mensajes recibido y de dicho código esperado; y

- cancelación de la autenticación, si el código de autenticación de mensajes recibido y el código esperado no coinciden.

Conforme con el invento existe también un paso adicional que es el siguiente:

- actualización en dicha primera entidad de un contador de fallos cada vez que el código de autenticación de mensajes recibido y el código esperado no coincidan después de una comparación por dicha primera entidad.

Dicho de otro modo, el invento consiste en proporcionar - dentro de la tarjeta USIM - un contador de fallos actualizado que depende del resultado de la comparación entre el MAC y XMAC para limitar el número sucesivo de intentos errados a una cantidad máxima, por encima de la cual la clave K no se considera segura. De esta manera, se controla el número sucesivo de ataques malintencionados.

Según las implementaciones preferidas, el método del invento puede incluir pasos adicionales como:

- verificación preliminar del contador de fallos por parte de dicha primera entidad antes de iniciar la autenticación,

- determinación por parte de dicha primera entidad, a partir de un número de secuencia incluido en dichos otros parámetros, si el código de autenticación de mensajes y otros parámetros han sido recibidos por dicha primera entidad; y si dicho número de secuencia indica que dicho código de autenticación de mensajes y los demás parámetros han sido recibidos por dicha primera entidad, se procede a la cancelación de la autenticación sin actualizar dicho contador de fallos,

- reajuste de dicho contador de fallos a su valor inicial, si (i) el código de autenticación de mensajes recibido y el código esperado coinciden y (ii) dicho número de secuencia indica que dicho código de autenticación de mensajes y otros parámetros aún no han sido recibidos por dicha primera entidad.

El presente invento también incluye una tarjeta inteligente adaptada para autenticar una entidad remota y los datos que se reciben de dicha entidad, la tarjeta inteligente incluye:

- una memoria que almacena algoritmos de autenticación, así como claves de cifrado y autenticación que incluyen una clave secreta idéntica a una clave correspondiente almacenada en la entidad remota;
- medios para recibir de dicha entidad remota un código de autenticación de mensajes y otros parámetros;
- medios para calcular un código esperado a partir de dichos otros parámetros y de dicha clave secreta;
- medios para comparar dicho código de autenticación de mensajes recibido y dicho código esperado; y
- medios para cancelar la autenticación, si el código de autenticación de mensajes recibido y el código esperado no coinciden.

De acuerdo con el invento dicha tarjeta inteligente comprende además:

- un contador de fallos adaptado para almacenar un número de incidencias de cancelación; y
- medios para actualizar el contador de fallos cada vez que los medios de comparación indiquen que el código de autenticación de mensajes y el código esperado no coinciden.

Por lo tanto, gracias a este contador de fallos incorporado y al hecho que la actualización del contador se controla desde el interior de la tarjeta, esta se convierte en un dispositivo más seguro y resistente a las alteraciones.

Breve descripción de los dibujos

Será posible entender mejor los objetivos, aspectos y ventajas del invento a través de la siguiente descripción detallada de una realización preferente del invento relacionada con los dibujos anexados.

La figura 1 ilustra un ejemplo de un sistema de procesamiento de datos en el cual se puede aplicar el invento.

La figura 2 es un ejemplo de un algoritmo de gestión del contador de fallos de autenticación.

Descripción detallada de una realización preferente del invento

La figura 1 ilustra un sistema que incluye un equipo de usuario que se comunica con un servidor SERV mediante una red NET como Internet o una red privada. El equipo de usuario consta de dos partes: el equipo móvil ME y el módulo de identidad del abonado CARD. El equipo móvil ME es el equipo radioeléctrico terminal utilizado para la radiocomunicación entre el equipo de usuario y el servidor SERV. En este ejemplo, la tarjeta CARD es una tarjeta inteligente USIM que contiene la identidad del abonado, ejecuta algoritmos de autenticación y almacena claves de cifrado y autenticación, así como información de subscripción necesaria en el terminal.

Se adapta el servidor SERV para proporcionar un servicio a una estación móvil tras la autenticación exitosa de dicha estación.

Conforme con el invento un contador en el interior de la tarjeta controla el número de procesos de autenticación cancelados por la tarjeta. Preferentemente, el contador cuenta los procesos de autenticación cancelados de manera sucesiva.

La figura 2 es un algoritmo de autenticación que ilustra el invento que incluye varios pasos S1-S16.

En un primer paso (S1), la tarjeta recibe una solicitud de autenticación.

Es un segundo paso (S2), antes de verificar el MAC, la tarjeta comprueba el contador de fallos:

- si el contador es cero (S3, S12), considera que la clave no es segura y no continúa el proceso. En este caso, la tarjeta devuelve un mensaje de error de seguridad (paso S14). El proceso de autenticación concluye tras el paso S14, (S 15);
- además (S3, S4) puede utilizar la clave y verificar (S5) los datos MAC proporcionados:
    - si el valor esperado por la tarjeta no coincide con el brindado en la solicitud, la tarjeta disminuye el contador de errores (S13) y envía una notificación de error de seguridad al ME.

- también verifica el SQN de la solicitud (S6) para garantizar que no está procesando una solicitud enviada previamente:
  - si el SQN no es reciente (S7, S10), la tarjeta envía un testigo de resincronización a la red (S10) tal y como se define en AKA. El proceso concluye (S11) tras S10;
  - asimismo, si el SQN es válido (S7, S8), en este ejemplo la tarjeta repone el contador de errores a su valor máximo (S8). Posteriormente, la tarjeta envía un resultado de autenticación positivo (S9). El paso S16 es el final del proceso de autenticación.

Cuando el contador de errores llega a cero, no se puede ya utilizar la clave de autenticación. Por consiguiente, sólo permite una pequeña cantidad de errores consecutivos. Los ataques mencionados requieren intentos que conducen a errores de verificación del MAC. Gracias a que el contador limita el número de intentos, se puede contrarrestar el ataque.

Por ejemplo, supongamos que el valor máximo del contador es 3 y el valor inicial es 1. Las siguientes seis autenticaciones consecutivas ilustran varios escenarios posibles.

1ª Autenticación: Contador > 0, MAC correcto, SQN válido

Valor inicial del contador: 1

- Recepción de la solicitud de autenticación (S1).
- Debido a que el contador es estrictamente positivo (S3), se efectúa una verificación del MAC (S4).
- Debido a que el MAC es correcto (S5), se efectúa una verificación del SQN (S6).
- Debido a que el SQN es válido (S7), se repone el contador a su valor máximo, por ejemplo 3 (S8).
- Se devuelve el resultado de la autenticación (S9).

Valor final del contador: 3

2ª Autenticación: Contador > 0, MAC incorrecto

Valor inicial del contador: 3

- Recepción de la solicitud de autenticación (S1).
- Debido a que el contador es estrictamente positivo (S3), se efectúa una verificación del MAC (S4).
- Debido a que el MAC es incorrecto (S5), el contador es disminuido. El nuevo valor del contador es 2 (S13).
- Se devuelve un mensaje de error de seguridad (S14).

Valor final del contador: 2

3ª Autenticación: Contador > 0, MAC correcto, SQN inválido

Valor inicial del contador: 2

- Recepción de la solicitud de autenticación (S1).
- Debido a que el contador es estrictamente positivo (S3), se efectúa una verificación del MAC (S4).
- Debido a que el MAC es correcto (S5), se efectúa una verificación del SQN (S6).
- Debido a que el SQN es inválido (S7), se envía un testigo de resincronización. El contador no es modificado. Continúa igual a 2.

Valor final del contador: 2.

4ª Autenticación: Contador > 0, MAC incorrecto

Valor inicial del contador: 2

- Recepción de la solicitud de autenticación (S1).
- Debido a que el contador es estrictamente positivo (S3), se efectúa una verificación del MAC (S4).
- Debido a que el MAC es incorrecto (S5), el contador es disminuido. El nuevo valor del contador. es 1 (S13)
- Se devuelve un mensaje de error de seguridad (S14).

Valor final del contador: 1

5ª Autenticación: Contador > 0, MAC incorrecto

Valor inicial del contador: 1

- Recepción de la solicitud de autenticación (S1).
- Debido a que el contador es estrictamente positivo (S3), se efectúa una verificación del MAC (S4).
- Debido a que el MAC es incorrecto (S5), el contador es disminuido. El nuevo valor del contador es 0 (S13).
- Se devuelve un mensaje de error de seguridad (S14).

Valor final del contador: 0

6ª Autenticación: Contador = 0, MAC incorrecto

Valor inicial del contador: 0

- Recepción de la solicitud de autenticación (S1).
- Debido a que el contador es igual a 0 (S3), la clave se bloquea (S12).
- Se devuelve un mensaje error de seguridad (S14).

Valor final del contador: 0

Las principales ventajas del invento son:

- el número de presentaciones de MAC incorrectos sucesivos se limita al valor máximo del contador (véanse las autenticaciones anteriores # 2,4,5,6);
- el número total de autenticaciones no es limitado ya que se puede reponer el contador a su valor máximo (véase la autenticación anterior # 1);
- la reiteración de una solicitud de autenticación correcta no repone el contador, debido a que el SQN es inválido necesariamente, y el contador permanecerá inalterable (véase la autenticación anterior # 3);
- los problemas asociados con la verificación del SQN no representan el riesgo de bloquear la tarjeta, ya que el contador no es disminuido (véase la autenticación anterior # 3);

Se deben consideran muchas variantes:

- los valores del contador son sólo un ejemplo;
- la gestión del contador puede diferir: el contador puede ser incrementado en lugar de disminuido, puede cambiar por incrementos de algún valor; puede ser comparado a algún valor distinto a 0 etc.;
- el contador puede contar la cantidad total de solicitudes de autenticación;
- el contador puede contar el número de MAC incorrectos sin posibilidades de reponerlo a su valor máximo;

- el contador puede ser repuesto tan pronto como el MAC sea correcto (es decir sin ninguna verificación adicional como la validez del SQN);

- el contador puede ser disminuido incluso si el MAC es correcto y el SQN es inválido.

REIVINDICACIONES

1. Un método de autenticación para ser utilizado en un sistema que incluye una primera entidad (CARD) y una segunda entidad (SERVER) comunicadas mediante una red (NET), donde la primera entidad se adapta para autenticar dicha segunda entidad y los datos que recibe de ésta; y donde ambas primera y segunda entidades poseen la misma clave secreta (K), dicho método de autenticación consta de los siguientes pasos:

- recepción por parte de dicha primera entidad de un código de autenticación de mensajes (MAC) y otros parámetros (RAND, SQN, AMF), siendo dicho código de autenticación de mensajes (MAC) una función de dicha clave secreta (K) y dichos otros parámetros (RAND, SQN, AMF);

- cálculo por parte de dicha primera entidad de un código esperado (XMAC) a partir de dichos otros parámetros que ya han sido recibidos y de dicha clave secreta (K) almacenada en dicha primera entidad;

- comparación por parte de dicha primera entidad de dicho código de autenticación de mensajes (MAC) recibido y dicho código esperado (XMAC); y

- cancelación de la autenticación, si el código de autenticación de mensajes (MAC) recibido y el código esperado (XMAC) no coinciden;

dicho método está **caracterizado** por los siguientes pasos:

- actualización en dicha primera entidad de un contador de fallos cada vez que el código de autenticación de mensajes (MAC) recibido y el código esperado (XMAC) no coinciden después de una comparación por dicha primera entidad.

- determinación por parte de dicha primera entidad, a partir de un número de secuencia (SQN) incluido en dichos otros parámetros, si el código de autenticación de mensajes (MAC) y los parámetros (RAND, SQN, AMF, etc.) han sido ya recibidos por dicha primera entidad; y

- si dicho número de secuencia (SQN) indica que dicho código de autenticación de mensajes (MAC) y otros parámetros (RAND, SQN, AMF, etc.) han sido recibidos por dicha primera entidad, se procede a la cancelación de la autenticación sin actualizar dicho contador de fallos.

2. El método conforme a la reivindicación 1, comprende además el siguiente paso:

- verificación preliminar del contador de fallos por parte de dicha primera entidad antes de iniciar la autenticación.

3. El método conforme a la reivindicación 1, comprende además el siguiente paso:

- reposición del contador de fallos a su valor inicial, si (i) el código de autenticación de mensajes (MAC) recibido y el código esperado coinciden y (ii) dicho número de secuencia (SQN) indica que dicho código de autenticación de mensajes (MAC) y otros parámetros (RAND, SQN, AMF, etc.) aún no han sido recibidos por dicha primera entidad.

4. Una tarjeta inteligente (CARD) adaptada para autenticar una entidad remota (SERV) y los datos recibidos de dicha entidad, dicha tarjeta inteligente incluye:

- una memoria que almacena algoritmos de autenticación, así como claves de cifrado y autenticación incluyendo una clave secreta (k) idéntica a una clave correspondiente almacenada en la entidad remota;

- medios para recibir de dicha entidad remota un código de autenticación de mensajes (MAC) y otros parámetros (RAND, SQN, AMF, etc.),

- medios para calcular un código esperado (XMAC) a partir de dichos otros parámetros y de dicha clave secreta (K);

- medios para comparar dicho código de autenticación de mensajes (MAC) recibido y dicho código esperado (XMAC); y

- medios para cancelar la autenticación y actualizar un contador de fallos, si el código de autenticación de mensajes (MAC) recibido y el código esperado (XMAC) no coinciden;

- medios para que dicha primera entidad pueda determinar, a partir de un número de secuencia (SQN) incluido en dichos otros parámetros, si dicho código de autenticación de mensajes (MAC) y otros parámetros (RAND, SQN, AMF, etc.) han sido ya recibidos por dicha primera entidad; y si dicho número de secuencia (SQN) indica que dicho código de autenticación de mensajes (MAC) y otros parámetros (RAND, SQN, AMF, etc.) han sido ya recibidos por dicha primera entidad, medios para proceder a la cancelación de la autenticación sin actualizar dicho contador de fallos.

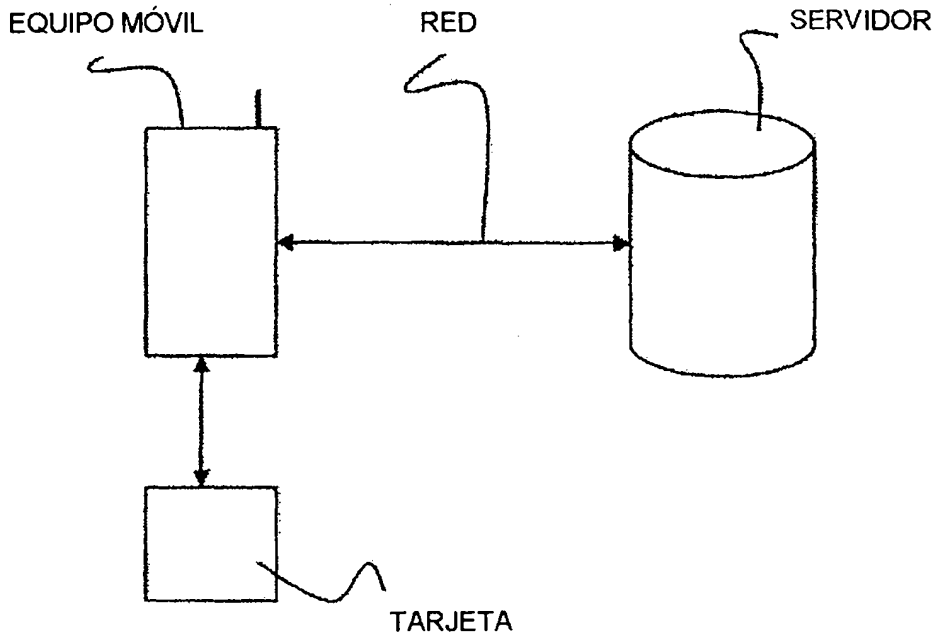

Figura 1

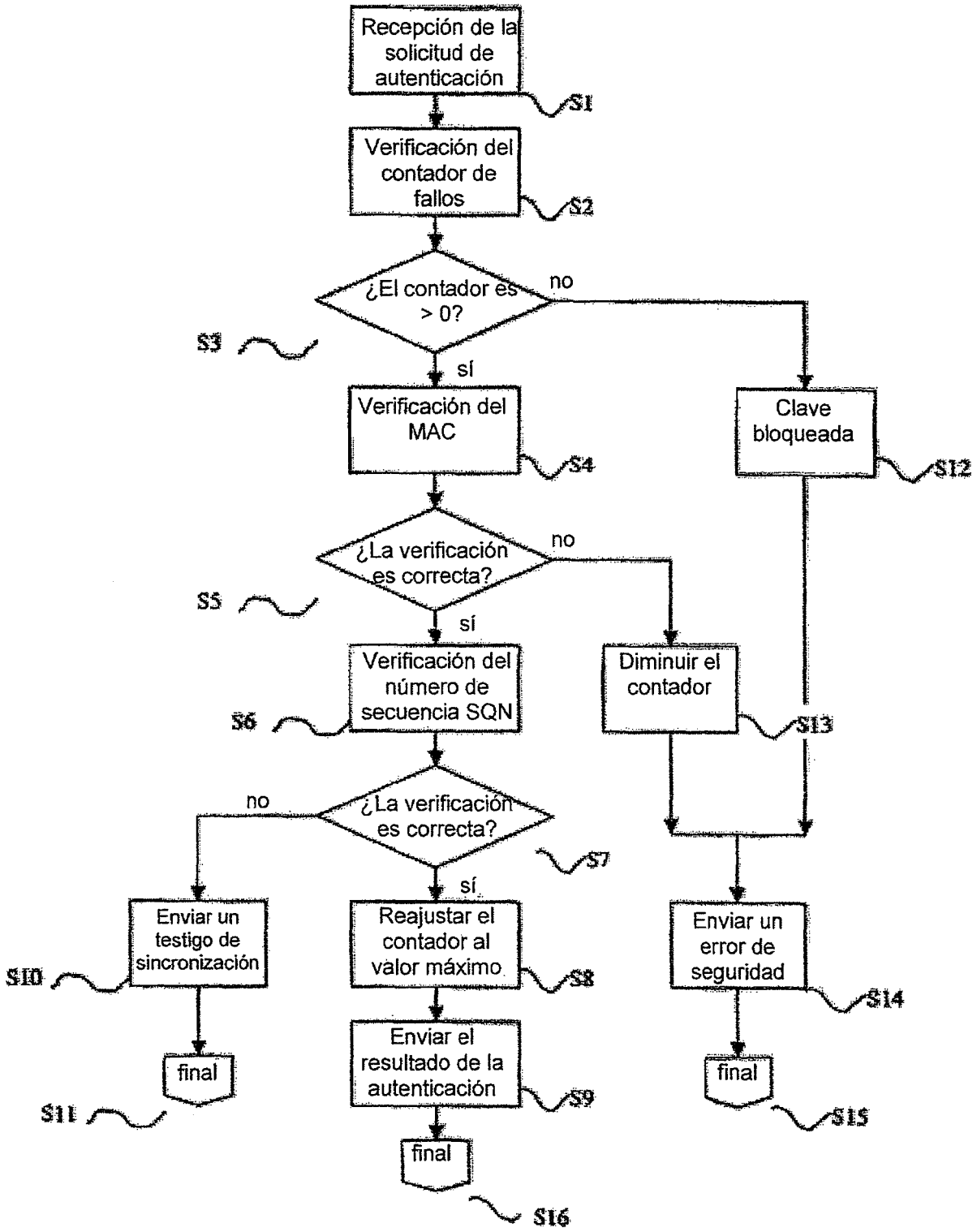
Recepción de la solicitud de autenticación
S1
Verificación del contador de fallos
S2
¿El contador es > 0?
no
S3
sí
Verificación del MAC
S4
Clave bloqueada
S12
¿La verificación es correcta?
no
S5
sí
Verificación del número de secuencia SQN
S6
Diminuir el contador
S13
¿La verificación es correcta?
no
S7
sí
Enviar un testigo de sincronización
S10
Reajustar el contador al valor máximo
S8
Enviar un error de seguridad
S14
final
S11
Enviar el resultado de la autenticación
S9
final
S15
final
S16

Figura 2