(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 759 340**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.06.2005 PCT/IB2005/001746**

(87) Fecha y número de publicación internacional: **05.01.2006 WO06000875**

(96) Fecha de presentación y número de la solicitud europea: **20.06.2005 E 05756710 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2019 EP 1769650**

(54) Título: **Método para asegurar un protocolo de autenticación y acuerdo de clave**

(30) Prioridad:

21.06.2004 EP 04291562

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.05.2020

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, Rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

SALGADO, STEPHANIE y
ABELLAN SEVILLA, JORGE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para asegurar un protocolo de autenticación y acuerdo de clave

La invención se refiere a redes de comunicaciones y, en particular, a protocolos de autenticación y acuerdo de clave en tales redes.

Técnica anterior

Los protocolos de autenticación y acuerdo de clave (AKA) se utilizan ampliamente en entornos cableados e inalámbricos para proporcionar material clave y prueba de la identidad entre dos entidades conectadas. Un ejemplo típico es un abonado inalámbrico que accede a una red celular que se autentica en un servidor de autenticación en la red.

Diferentes entidades o dispositivos están involucrados en un procedimiento de AKA.

Un terminal HT que aloja un componente léxico personal (por ejemplo, un teléfono móvil) y un servidor de autenticación (AS) se comunican entre sí. El componente léxico personal y un servidor seguro almacenan una misma clave secreta K, también conocida como la clave maestra.

En el protocolo AKA habitual (por ejemplo, para implementar una transferencia de datos segura), tanto el servidor de autenticación como el terminal de alojamiento HT son capaces de utilizar claves derivadas de una clave maestra, es decir de una clave de integridad Ik y una clave de cifrado Ck. Tales claves Ik y Ck se derivan de una clave maestra que es compartida por un servidor seguro por un lado y el componente léxico personal por otro lado.

En otras circunstancias, es decir un procedimiento AKA especial, el terminal de alojamiento puede verse privado del uso tanto de la clave de integridad Ik como de la clave de cifrado Ck, es decir, estas claves derivadas se consideran datos confidenciales que no deben revelarse al terminal de alojamiento.

El procedimiento para realizar un procedimiento AKA habitual se describirá ahora con referencia a la figura 1.

Típicamente, un servidor seguro SS elige una matriz aleatoria RAND. Utilizando la RAND con un algoritmo llamado AKAAlg y la clave secreta K que es compartida solamente por el servidor seguro SS y el componente léxico personal, el servidor seguro SS produce un vector de autenticación (AV).

El vector de autenticación AV se compone al menos de los siguientes componentes: la RAND inicial, un valor de resultado (RES), algún material de clave derivada (DKM) es decir, típicamente las claves derivadas Ik y Ck, y un código de autenticación de mensaje (MAC). El vector de autenticación AV se entrega a continuación al servidor de autenticación AS.

El servidor de autenticación AS envía los valores de la RAND, los valores MAC y posiblemente otros datos al terminal de alojamiento HT. El terminal de alojamiento a continuación los envía al componente léxico personal SE.

El componente léxico personal SE ejecuta el algoritmo AKAAlg utilizando la clave secreta K almacenada y los parámetros recibidos (al menos la RAND, MAC).

El componente léxico personal SE vuelve a calcular un MACT según la clave secreta K compartida, y según la RAND recibida.

El componente léxico personal SE a continuación compara el valor MACT nuevamente calculado con el valor MAC recibido (¿es MAC = MACT?) con el fin de realizar alguna comprobación de integridad y posiblemente un procedimiento de autenticación del servidor de autenticación.

Después el componente léxico personal SE calcula RES.

El terminal de alojamiento envía RES al servidor de autenticación de manera que el servidor autentique el componente léxico personal. Al final, el servidor de autenticación AS autentica el componente léxico personal comparando el RES recibido del terminal de alojamiento con el valor XRED recibido del servidor seguro SS.

El componente léxico personal SE también calcula las claves derivadas Ik y Ck y las envía junto con RES al terminal de alojamiento. El terminal de alojamiento utiliza las claves derivadas para realizar cualquier operación de seguridad adicional hacia el AS.

Un ejemplo de este procedimiento básico AKA de autenticación es UMTS AKA como se define en 3GPP TS 33.102.

El procedimiento habitual de AKA explicado está bien adaptado para proporcionar autenticación segura y compartir material clave entre el terminal de alojamiento HT y el servidor de autenticación AS. Sin embargo, en algunas circunstancias específicas, es necesario que el algoritmo AKAAlg se procese de manera diferente dentro del componente léxico personal. Por ejemplo, en algunas circunstancias específicas, se requiere que las claves derivadas Ik y Ck o parte de ellas se consideren como datos confidenciales y, por lo tanto, se impida que se revelen

al terminal de alojamiento, es decir que las claves derivadas Ik y Ck se mantengan dentro del componente léxico personal en lugar de entregarse al terminal de alojamiento.

En estos casos específicos, un requisito básico para muchas situaciones es que el terminal de alojamiento no podría recuperar las claves derivadas utilizando el AKA estándar o cualquier otro procedimiento.

El documento "Security architecture and mechanism of third generation mobile comunication" ("Arquitectura y mecanismo de seguridad de comunicación móvil de tercera generación") de MIN LEI Y COL. IEEE TENCON' O2.2002 IEEE REGION 10 CONFERENCE ON COMPUTERS, COMMUNICATIONS,M CONTROL AND POWER ENGINEERING PROCEEDINGS. BEIJING, CHINA, OCT. 28-31, 2002, IEEE REGION 10 ANNUAL CONFERENCE, NEW YORK, NY: IEEE, US, vol. VOL. 1 de 3, 28 de Octubre de 2002 (2002-10-28), páginas 813-816, XP010627367, ISBN: 0-7803-7490- describe en UMTS AKA estándar.

El documento "Payphone service for third generation mobile systems" ("Servicio de teléfono público para sistemas móviles de tercera generación") por KRAYEM-NEVOUX R Y COL., GLOBAL TELECOMMUNICATIONS CONFERENCE, 1993, INCLUDING A COMMUNICATIONS THEORY MINI-CONFERENCE., IEEE IN HOUSTON GLOBECOM '93., IEEE HOUSTON, TX, USA 29 NOV.- 2 DIC. 1993, NEW YORK, NY, USA, IEEE, 29 DE Noviembre de 1993 (1993-11-29), páginas 1708-1712, XP010109936, ISBN: 0-7803-0917-0, por otro lado, describe un esquema de autenticación y configuración de clave para sistemas móviles de tercera generación en donde las claves criptográficas se mantienen en almacenamiento comparativamente seguro en un módulo de usuario (es decir una tarjeta IC). El teléfono móvil, que está separado del módulo de usuario (o "elemento seguro"), no recibe el material clave criptográfico.

El objetivo de la invención es proporcionar una solución para evitar la revelación de las claves derivadas al terminal de alojamiento.

De manera más general, existen algunos procedimientos de autenticación específicos que se basan en el procedimiento AKA habitual pero que difieren en algunos aspectos que pueden ser de cualquier tipo. Un mismo componente léxico personal puede estar sujeto a diferentes reacciones según los diferentes procedimientos AKA posibles encontrados durante su vida útil.

Un segundo objetivo de la invención es proponer una forma de señalizar eficientemente que se requiere un procedimiento de autenticación particular para el componente léxico personal.

Breve descripción de los dibujos

Otros propósitos, características y ventajas de la invención aparecerán en la lectura de la descripción que sigue de una implementación preferida de la invención y de una realización de un sistema diseñado para esta implementación, dado como un ejemplo no limitativo, y que hace referencia a los dibujos adjuntos en los que:

la figura 1 es una vista esquemática de diferentes etapas de un procedimiento AKA conocido;

la figura 2 es una vista esquemática de diferentes etapas de un procedimiento según la presente invención basada en AKA.

Mejor forma de realizar la invención

El sistema según la presente invención, como se ve en la figura 2, comprende diferentes entidades o dispositivos, los mismos que los involucrados en un procedimiento de AKA.

El sistema comprende un terminal HT que aloja un componente léxico personal SE. En una realización particular, el terminal de alojamiento HT puede ser un teléfono móvil o, más generalmente, un dispositivo de aceptación de componente léxico personal; el dispositivo de aceptación de componente léxico personal puede tener la forma de un alojamiento provisto de una abertura o ranura para recibir el componente léxico personal, pero también cualquier forma que permita que el componente léxico personal se comunique con el dispositivo de aceptación de componente léxico personal;

El sistema comprende un servidor de autenticación AS y un servidor seguro SS con el que se comunica el servidor de autenticación y en cuyo servidor seguro se mantiene una clave secreta o una clave maestra K;

El componente léxico personal o elemento seguro SE está alojado en el terminal HT. El terminal de alojamiento HT se comunica con el componente léxico.

La clave secreta K también se mantiene en el componente léxico pero no se revela al terminal de alojamiento HT. Como es bien sabido, la clave secreta K es un secreto compartido entre el componente léxico personal y el servidor seguro.

En una realización particular, el componente léxico personal (SE) es una tarjeta con circuito integrado también llamada tarjeta inteligente.

La presente invención consiste en asegurar un procedimiento de autenticación y acuerdo de clave (AKA), es decir un procedimiento que permite establecer material clave y proporcionar una prueba de la identidad entre dos entidades conectadas.

La presente realización permite evitar la revelación de claves derivadas tales como la clave de integridad Ik o la clave de cifrado Ck al terminal de alojamiento HT, es decir para evitar la revelación de material de clave derivada o parte de éste, al terminal de alojamiento HT.

El procedimiento según la presente realización comprende las siguientes etapas:

El terminal de alojamiento HT envía una solicitud HTTP hacia el servidor de autenticación, solicitando un procedimiento AKA. El procedimiento de AKA también puede ser solicitado por el servidor de autenticación.

El AS se proporciona con un vector de autenticación (AV) estándar del Servidor seguro (SS) (etapa 1 en la figura 2).

El vector de autenticación (AV) se compone al menos de los siguientes componentes: la RAND inicial, un valor de resultado RES y el material de clave derivada referenciado DKM en lo siguiente, es decir claves derivadas Ik y Ck, y un código de autenticación de mensaje (MAC).

El servidor de autenticación AS determina si la modificación del MAC es necesaria o no según la naturaleza del componente léxico personal encontrado (también llamado componente léxico de autenticación), y en particular basándose en la configuración de seguridad del usuario (USS) asociada con el componente léxico personal encontrado Tales configuraciones pueden almacenarse previamente en el lado del servidor de autenticación, o pueden recibirse desde el componente léxico personal a través del terminal HT.

Para algunos tipos de componentes léxicos personales para los que Ik y Ck no se consideran datos confidenciales, se debe aplicar el procedimiento AKA habitual, es decir, el MAC no modificado se transmitirá al componente léxico con el valor de la RAND, y las claves derivadas se transmitirán a continuación mediante el componente léxico personal al terminal de alojamiento HT.

Sin embargo, debería ocultarse las claves derivadas según las configuraciones de seguridad del usuario, el servidor de autenticación AS toma el valor MAC del vector de autenticación AV y calcula una modificación de dicho MAC utilizando una de las claves derivadas. El Mac se modifica así, utilizando al menos parte del material de clave derivada DKM.

Como ejemplo de tal modificación del MAC utilizando material de clave derivada, esta modificación puede ser MAC* = M(MAC, DKM*) donde DKM* es una parte modificada del material de clave derivada DKM, por ejemplo, un valor Ik* modificado basándose en el valor de la clave de integridad Ik.

Tanto la clave de integridad Ik como la Clave de Cifrado Ck se derivan de la clave maestra K y de la RAND mediante un cálculo realizado por el servidor seguro.

Como se explicará más adelante, dicha clave maestra secreta K también se almacena en el componente léxico personal SE y tal derivación también es posible en el componente léxico personal siempre que el componente léxico haya recibido la RAND. La clave maestra K, por lo tanto, constituye un secreto compartido entre el componente léxico personal y el servidor seguro.

Basándose en una de las claves derivadas que Ik y Ck recibieron del servidor seguro SS, el servidor de autenticación AS calcula una modificación, al menos de parte del material de clave derivada, es decir, calcula el parámetro DKM* expresado aquí arriba. Por ejemplo, el servidor de autenticación AS toma los primeros 64 bits de la función (sha - 1) bien conocida aplicada a la clave de integridad Ik.:

$$Ik^* = Trunc(SHA\text{-}1\ (IK))$$

Trunc indica el truncamiento en la salida de bit de (SHA-1) y (SHA-1) es una función hash bien conocida aplicada a la clave de integridad Ik.

MAC* se puede calcular de la siguiente manera (etapa 3 en la figura 2):

$$MAC^* = MAC\ XOR\ Trunc(SHA\text{-}1\ (IK))$$

La modificación del MAC es preferiblemente reversible dependiendo del conocimiento de dicha parte modificada del material de clave derivada DKM*, en la fórmula MAC* = MAC XOR DKM*;

Una vez que el servidor de autenticación AS calcula el valor modificado MAC*, el servidor de autenticación AS envía la RAND junto con el MAC* y junto con valores tales como SQN, AK, AMF al terminal de alojamiento HT (etapa 4 en la figura 2). Por ejemplo, se utiliza un mismo mensaje para enviar esos datos diferentes.

El valor RES permanece almacenado en el servidor de autenticación.

El terminal de alojamiento HT a continuación envía la RAND, MAC*, SON, AK, AMF (y posiblemente otros valores) al componente léxico personal SE (etapa 5 en la figura 2).

Se realiza un algoritmo AKAAIg adicional en el componente léxico personal SE de la siguiente manera:

El componente léxico personal SE calcula las claves derivadas Ck, Ik y el valor RES, cuyos cálculos son posibles en el componente léxico personal porque el componente léxico personal almacena la clave maestra K y acaba de recibir la RAND que es necesario tanto para calcular Ck y Ik como para calcular RES.

En este momento, Ck e Ik están presentes en el servidor de autenticación AS y en el componente léxico personal SE, pero no en el terminal de alojamiento HT. Hasta entonces, estas claves Ck e Ik pueden considerarse datos confidenciales porque no se divulgan al terminal de alojamiento HT.

En el presente ejemplo, el componente léxico personal realiza el cálculo del MAC no modificado sobre la base del MAC* recibido y sobre la base del Ik nuevamente calculado.

Para este fin, el componente léxico personal SE calcula la clave de integridad Ik* modificada, es decir la parte modificada DKM* del material de clave derivada DKM.

$$Ik^* = Trunc(sha - 1 (Ik))$$

A continuación el componente léxico personal calcula el valor MAC correspondiente al valor modificado MAC* recibido:

MACC = M'(MAC*, Ik*), es decir MACC = M'(MAC*, DKM*) donde M' es la función inversa de M utilizada por AS, es decir, MACC = MAC* XOR Ik* en el presente caso (etapa 6 en la figura 2). La función reversible M' es conocida de antemano tanto por el componente léxico personal SE como por el servidor de autenticación AS.

El cálculo de M' es, en el ejemplo detallado dado anteriormente, el siguiente cálculo: MACC = MAC* XOR Trunc(SHA-1 (IK))

El componente léxico también calcula MACT, es decir, el valor de MAC calculado sobre la base tanto de LA RAND como de la clave maestra K. Típicamente, el MAC dependerá también de los parámetros transmitidos SQN y AMF.

MACT a continuación se compara con MACC (etapa 7 en la figura 2).

Como se ha descrito anteriormente, M es preferiblemente una función reversible, mientras que la clave derivada utilizada en el cálculo del MAC modificado se conoce en ambos lados.

M puede no ser reversible. En tal caso, el componente léxico personal vuelve a calcular el valor MAC, a continuación vuelve a calcular la modificación del valor MAC y después compara el valor modificado MAC recibido con el valor MAC nuevamente calculado y modificado nuevamente.

Una forma de comparar MACC con MACT es comparar una concatenación de MACT con otros valores, por ejemplo comparar (SQN xor AK || AMF || MACT) con una concatenación de MACT con otros valores, por ejemplo (SQN xor AK || AMF || MACC), en cuyas fórmulas || es el símbolo de concatenación.

En caso de que la comparación MAC no tenga éxito, es decir, MACT parece ser diferente de MACC, el componente léxico personal informa al terminal de alojamiento HT que la comparación MAC no ha tenido éxito.

En caso de que la comparación MAC tenga éxito, el componente léxico personal SE calcula y envía RES al terminal de alojamiento (etapa 8 en la figura 2) y mantiene ocultos los otros datos (DKM, es decir, Ik y Ck en el presente ejemplo) o una parte de ellos ocultos en el componente léxico. El terminal de alojamiento a continuación envía RES al servidor de autenticación AS (etapa 9 en la figura 2) para la autenticación del componente léxico personal SE por el servidor de autenticación AS.

En el presente ejemplo, tanto el componente léxico personal SE como el servidor de autenticación AS utilizarán una concatenación de Ik y Ck llamada Ks para derivar claves específicas de NAF interna y externa Ks_ ext_NAF y Ks_int_NAF.

La clave específica de NAF interna Ks_int_NAF se utiliza para establecer un canal seguro entre el componente léxico personal y un servidor remoto a través del terminal HT pero oculto del terminal HT.

La clave específica de NAF externa Ks_ext_NAF se utiliza para establecer un canal seguro entre el terminal de alojamiento HT y un servidor remoto.

En el caso de que el servidor de autenticación AS no modifique el MAC antes de enviarse al componente léxico personal SE a través del terminal, el componente léxico personal SE se comporta según el procedimiento habitual, es decir, vuelve a calcular y comprueba el valor del MAC y, después de la autenticación, proporciona las claves derivadas Ik y Ck al terminal.

Tal modificación del MAC o de cualquier otro dato asociado con la RAND en el procedimiento de autenticación mediante el uso de material de clave derivada o parte de éste, proporciona muchas ventajas por sí mismo, independientemente de la posibilidad de desencadenar un procedimiento especial entre los dos proporcionados.

Es por eso que la modificación del MAC puede aplicarse sistemáticamente sin posibilidad de diferentes procedimientos dependiendo de la modificación o no del MAC.

La modificación del MAC tiene la ventaja de ocultar el verdadero valor del MAC, impidiendo por ello cualquier interpretación del MAC con la RAND asociada por una entidad fraudulenta que a continuación puede deducir algún valor de los datos sensibles.

Aunque oculto por tal modificación, sin embargo el MAC sigue siendo capaz de ser interpretado por el componente léxico personal, es decir, el componente léxico aún puede comprobar la validez del MAC, ya que el componente léxico personal incorpora el material de clave derivada que es necesario para comprobar tal validez.

La modificación del MAC también tiene la ventaja de impedir que una entidad fraudulenta pueda recoger una pareja transmitida (RAND, MAC) y pueda reproducirla en el componente léxico, con el fin de obtener el valor de Ck e Ik a cambio.

Todas estas ventajas también son válidas para otros datos transmitidos con la RAND.

Independientemente de las ventajas ocultas explicadas anteriormente, la posibilidad de optar o no por la modificación del MAC o de otros datos transmitidos con la RAND en el procedimiento de autenticación tiene la ventaja de señalar de manera eficiente un procedimiento especial que la tarjeta debe realizar en respuesta a tal modificación.

En el presente caso, tal modificación del MAC señala la necesidad de mantener los datos confidenciales Ik y Ck dentro de la tarjeta. Se puede aplicar la misma señalización para indicar un procedimiento particular que se llevará a cabo en el componente léxico, cualquiera que sea el procedimiento que puede ser diferente de ocultar el material de clave derivada. El componente léxico puede interpretar que un MAC modificado desencadena un comportamiento especial a realizar por el componente léxico en respuesta a dicha señalización.

También en el caso de ocultar el material de clave derivada, la señalización a través de la modificación puede consistir en inducir al componente léxico a consultar un indicador tal como el parámetro AMF que se envía al componente léxico junto con la RAND. El componente léxico a continuación puede leer un valor especial del AMF como un significado particular, por ejemplo, ordenar la ocultación de Ck e Ik mediante el componente léxico o cualquier otro procedimiento. En ausencia de tal MAC modificado y, por lo tanto, de cualquier redirección al indicador AMF, se le permitirá a la misma tarjeta revelar los valores Ck e Ik.

En tal ejemplo, existen muchas combinaciones entre el significado del MAC que es modificado o no y el valor particular del indicador AMF en cuyo indicador el componente léxico es redirigido por el MAC que es modificado.

Se pueden aplicar los mismos procedimientos descritos anteriormente utilizando una modificación de cualquier valor que se transmite con la RAND. Tal otro valor como el MAC puede ser un valor que se utiliza en el cálculo del MAC. Sin embargo, tal valor preferiblemente no se utiliza en el cálculo de ningún material de clave derivada.

Tales otros datos que pueden modificarse pueden ser el SQN como un ejemplo. El SQN puede modificarse de la siguiente manera:

El servidor de autenticación modifica el SQN, por ejemplo de la siguiente manera: SQN* = SQN XOR DKM* y después transmite la RAND, SQN* y el MAC no modificado (calculado por el SS a partir del valor SQN no modificado y la RAND). A continuación, el componente léxico realiza las siguientes operaciones.

Primero, el componente léxico comprueba que el SQN recibido (ya sea el SQN no modificado o el SQN* modificado) esté en un intervalo correcto según las reglas de administración de SQN.

En segundo lugar, el componente léxico administra dos casos posibles. En el primer caso, el componente léxico supone que SQN no se ha modificado.

A continuación, el componente léxico comprueba que SQN esté en el intervalo correcto. En el caso de que SQN esté en el intervalo correcto, entonces el componente léxico calcula MACT como una función de la RAND, la clave maestra y típicamente el SQN y el AMF y compara MACT con el MAC recibido. El valor MAC se calcula preferiblemente con los datos no modificados, es decir la RAND, SQN y AMF no modificados.

Si MAC = MACT, entonces el componente léxico identifica que está teniendo lugar el AKA habitual y así, se revelan CK y DK.

De lo contrario, el componente léxico administra el segundo caso.

El componente léxico supone que SQN se ha modificado y así, que SQN* era el valor recibido.

A continuación, el componente léxico calcula DKM, calcula DKM*, calcula SQN = SQN* XOR DKM*, calcula MACT como una función de la clave maestra, la RAND, y típicamente el SQN y el indicador AMF y a continuación compara MACT con el MAC recibido.

Si MACT es diferente de MAC, entonces la autenticación se rechaza.

De lo contrario, el componente léxico verifica que SQN está en el intervalo correcto y después no revela CK e IK.

SQN o SQN* pueden enviarse ocultos por AK (así, se envía SQN xor AK o SQN xor DKM* xor AK).

AMF se puede modificar al mismo tiempo que SQN, por ejemplo, realizando SQN_AMF* = (SQN || AMF) xor DKM*.

SQN, AMF y MAC también se pueden modificar al mismo tiempo que AUTH* = (SQN || AMF || MAC) xor DKM*.

Sin embargo, la RAND no debería modificarse, ya que se utiliza para calcular DKM.

Se puede aplicar la misma señalización para indicar al terminal de alojamiento a través de la tarjeta que se debe imponer un uso específico en cuanto a algunos datos confidenciales, típicamente en cuanto al material de clave derivada. En este caso, aún cuando el material de clave derivada sale del SE, el terminal de alojamiento puede realizar los procedimientos MAC descritos por sí mismo después de que el AKAAIg haya tenido lugar en el componente léxico personal.

REIVINDICACIONES

1.- Un método para asegurar un procedimiento de autenticación y acuerdo de clave en una red que incluye un servidor seguro, un servidor de autenticación y al menos un terminal (HT) que aloja un componente léxico personal (SE), comprendiendo dicho método de autenticación las siguientes etapas:

a. En el servidor seguro, realizar un cálculo sobre la base de datos aleatorios (RAND) y una clave secreta, produciendo por tanto material de clave derivada (Ck, Ik);

b. Enviar dicho material de clave derivada (Ck, Ik) junto con dichos datos aleatorios y junto con primeros datos (AUTN, XRES, MAC, SQN, Ak, AMF) desde el servidor seguro (SS) al servidor de autenticación (AS);

c. en dicho servidor de autenticación, generar segundos datos (MAC*, SQN*) modificando al menos parte de dichos primeros datos por medio de al menos parte de dicho material de clave derivada (Ck, Ik),

d. Enviar dichos segundos datos y dichos datos aleatorios (RAND) a través del terminal de alojamiento a dicho componente léxico personal;

e. En el componente léxico personal, realizar un cálculo basándose en los datos aleatorios (RAND) recibidos para volver a calcular al menos dicha parte de dicho material de clave derivada (Ck, Ik) tal como se utiliza en el servidor de autenticación para modificar dicha parte de primeros datos;

f. En el componente léxico, utilizar dicho nuevo cálculo al menos de parte del material de clave derivada para interpretar la parte modificada de los segundos datos recibidos.

g1. Si dicha parte de los segundos datos se ha modificado con al menos dicha parte del material de clave derivada, mantener en el componente léxico al menos una porción del material de clave derivada manteniéndolo oculto en el componente léxico.

2.- El método según la reivindicación 1, caracterizado porque dicha interpretación de la parte modificada de los segundos datos recibidos incluye identificar si dicha parte de los segundos datos recibidos se ha modificado o no antes de enviar tales segundos datos al componente léxico personal.

3.- El método según la reivindicación 1, caracterizado porque dicha interpretación de la parte modificada de los segundos datos recibidos incluye comprobar la validez de un valor esperado para los segundos datos recibidos.

4.- Un método según la reivindicación 1, caracterizado porque dicha parte nuevamente calculada del material de clave derivada se mantiene en la ficha personal manteniéndolo oculto en el componente léxico.

5.- El método según la reivindicación 1, caracterizado porque dicho método incluye el componente léxico que realiza un nuevo cálculo de dicha parte de los primeros datos sobre la base de dichos datos aleatorios recibidos y realiza una nueva modificación de dicha parte de los primeros datos sobre la base de dicho material de clave derivada, y la comparación de la parte de nuevo cálculo y primeros datos modificados de nuevo con la parte modificada recibida de los segundos datos.

6.- El método según la reivindicación 1, caracterizado porque incluye el componente léxico que realiza una modificación inversa de la parte modificada recibida de los segundos datos así como para recuperar la parte no modificada de los primeros datos como se ha producido inicialmente por el servidor seguro, volviendo a calcular en el componente léxico dicha parte de los segundos datos sobre la base de dichos datos aleatorios recibidos y sobre la base de la clave secreta, y realizando una comparación de la parte no modificada de los primeros datos como se ha producido inicialmente por el servidor seguro con la parte nuevamente calculada de los primeros datos.

7.- El método según cualquiera de las reivindicaciones precedentes, caracterizado porque dicha parte modificada de los segundos datos es el MAC (Código de autenticación de mensaje) como se utiliza generalmente para autenticar un servidor en el componente léxico.

8.- El método según la reivindicación precedente, caracterizado porque el componente léxico realiza un nuevo cálculo del MAC.

9.- El método según la reivindicación precedente, caracterizado porque el componente léxico personal realiza una modificación del MAC nuevamente calculado basándose en el material de clave derivada y compara dicho MAC nuevamente calculado modificado con el MAC modificado recibido del servidor de autenticación a través del terminal de alojamiento.

10.- El método según cualquiera de las reivindicaciones 7 a 9, caracterizado porque el componente léxico utiliza el material de clave derivada para realizar una modificación inversa del MAC modificado recibido y compara el MAC nuevamente calculado con el MAC recibido inversamente modificado.

11.- El método según cualquiera de las reivindicaciones previas, caracterizado porque el material de clave derivada

incluye al menos una parte de la clave de cifrado (Ck).

12.- El método según cualquiera de las reivindicaciones previas, caracterizado porque al menos dicha parte del material de clave derivada incluye la clave de integridad (Ik).

13.- El método según cualquiera de las reivindicaciones precedentes, caracterizado porque incluye las siguientes etapas:

g2) si dicha parte de los segundos datos no se ha modificado, trasmitiendo desde el componente léxico al terminal dicha porción del material de clave derivada.

14.- El método según la reivindicación 13, caracterizado porque dicho método incluye el componente léxico personal que realiza un nuevo cálculo de dicha parte de los segundos datos sobre la base de dichos datos aleatorios recibidos y el componente léxico personal que mantiene dicha porción del material de clave derivada dentro del componente léxico en caso de que dicha parte recibida de los segundos datos no corresponda ni a la parte nuevamente calculada de los segundos datos, ni a dicha parte nuevamente calculada de los segundos datos como modificada nuevamente con el material de clave derivada.

15.- El método según cualquiera de las reivindicaciones previas, caracterizado porque el componente léxico personal envía a través del terminal una respuesta (RES) al servidor de autenticación y el servidor de autenticación autentica el componente léxico personal por medio de dicha respuesta, y en eso una vez que el servidor de autenticación y el componente léxico personal se autentican mutuamente, el componente léxico personal deriva una clave interna (KsNAFint) y una clave externa (KsNAFext) del material de clave derivada (Ck, Ik), siendo utilizada dicha clave interna (KsNAFint) para establecer un canal seguro entre el componente léxico personal y un servidor remoto a través del terminal pero oculto al terminal, y siendo utilizada dicha clave externa (KsNAFext) para establecer un canal seguro entre el terminal y un servidor remoto.

16.- Un método de autenticación en una red que incluye un servidor seguro, un servidor de autenticación y al menos un terminal que aloja un componente léxico personal, comprendiendo dicho método de autenticación las siguientes etapas:

a. En el servidor seguro, realizar un cálculo sobre la base de unos datos aleatorios (RAND) y una clave secreta para producir el material de clave derivada (Ck, Ik);

b. Enviar dicho material de clave derivada (Ck, Ik) junto con dichos datos aleatorios y junto con unos primeros datos (AUTN, XRES, MAC, SQN, Ak, AMF) desde el servidor seguro (SS) al servidor de autenticación (AS);

b'. En dicho servidor de autenticación, utilizar una base de datos de los componentes léxicos personales en la red para determinar si el componente léxico a autenticar es un primer componente léxico personal o un segundo tipo de componente léxico personal.

En el caso de que el componente léxico sea un componente léxico personal de primer tipo:

c1. Generar unos segundos datos (MAC*, SQN*) modificando al menos parte de dichos primeros datos por medio al menos de parte de dicho material de clave derivada (Ck, Ik),

d1. Enviar dichos segundos datos y dichos datos aleatorios (RAND) a través del terminal de alojamiento a dicho componente léxico personal;

e1. En el componente léxico personal, volver a calcular al menos dicha parte de dicho material de clave derivada (Ck, Ik) sobre la base de los datos aleatorios RAND recibidos y la clave secreta K;

f1. En el componente léxico, utilizar dicho nuevo cálculo al menos de parte del material de clave derivada para interpretar la parte modificada de los segundos datos recibidos;

g1. Mantener en el componente léxico dicha parte nuevamente calculada del material de clave derivada manteniéndola oculta en el componente léxico.

c2. Enviar dichos segundos datos y dichos datos aleatorios (RAND) a través del terminal de alojamiento a dicho componente léxico personal sin realizar dicha modificación basándose en dicha parte del material de clave derivada,

d2. En el componente léxico personal, volver a calcular al menos dicha parte de dicho material de clave derivada (Ck, Ik) sobre la base de los datos aleatorios RAND recibidos y la clave secreta K y transmitir desde el componente léxico personal al terminal al menos dicha parte del material de clave derivada.

17.- Un componente léxico personal para un terminal en una red de comunicación que incluye un servidor de autenticación y un servidor seguro que produce material de clave derivada sobre la base de datos aleatorios y una clave secreta (K), incluyendo dicho componente léxico personal instrucciones de programa para volver a calcular el material de clave derivada (Ck, Ik) sobre la base de los datos aleatorios (RAND) recibidos y la clave secreta (K)

como se ha almacenado en el componente léxico personal, caracterizado porque el componente léxico personal incluye instrucciones del programa para utilizar una parte nuevamente calculada del material de clave derivada con el fin de interpretar los segundos datos recibidos, si dicha parte de los segundos datos se ha modificado al menos con dicha parte del material de clave derivada, que mantiene en el componente léxico al menos una porción del material de clave derivada manteniéndola oculta en el componente léxico.

18.- El componente léxico personal según la reivindicación 17, caracterizado porque incluye instrucciones de programa para mantener el material de clave derivada nuevamente calculado en el componente léxico personal manteniéndolo oculto en el componente léxico.

19.- El componente léxico personal según la reivindicación 17, caracterizado porque el componente léxico incluye instrucciones de programa para realizar nuevamente el cálculo de dicha parte de los primeros datos sobre la base de dichos datos aleatorios (RAND) recibidos, modificando nuevamente dicha parte sobre la base de dicha parte del material de clave derivada y comparando la parte de primeros datos nuevamente calculados y modificados con la parte modificada recibida de los segundos datos.

20.- El componente léxico personal según la reivindicación 17, caracterizado porque el componente léxico incluye instrucciones de programa para realizar una modificación inversa de la parte modificada recibida de los datos adicionales así como para recuperar la parte no modificada de los primeros datos producida inicialmente por un servidor seguro, volviendo a calcular dicha parte de los primeros datos sobre la base de dichos datos aleatorios (RAND) recibidos y sobre la base de la clave secreta (K), y comparando la parte no modificada de los segundos datos como se ha producido inicialmente por el servidor seguro con el parte nuevamente calculada de los segundos datos.

21.- El componente léxico personal según la reivindicación 17, caracterizado porque dicha parte modificada de los segundos datos es el MAC (Código de autenticación de mensaje) como se utiliza generalmente para autenticar un servidor en el componente léxico.

22.- El componente léxico personal según la reivindicación precedente, caracterizado porque el componente léxico realiza un nuevo cálculo del MAC.

23.- El componente léxico personal según la reivindicación 21, caracterizado porque el componente léxico personal realiza una modificación del MAC nuevamente calculado basándose en dicha parte del material de clave derivada y compara dicho MAC nuevamente calculado y modificado con el MAC modificado recibido del servidor de autenticación a través de la terminal de alojamiento.

24.- El componente léxico personal según la reivindicación 21, caracterizado porque el componente léxico utiliza dicha parte del material de clave derivada para realizar una modificación inversa del MAC modificado recibido y compara el MAC nuevamente calculado con el MAC recibido inversamente modificado.

25.- El componente léxico personal según cualquiera de las reivindicaciones 17 a 24, caracterizado porque el material de clave derivada incluye al menos una parte de la clave de cifrado (Ck).

26.- componente léxico personal según cualquiera de las reivindicaciones previas, caracterizado porque el material de clave derivada incluye al menos una parte de la clave de integridad (Ik).

27.- El componente léxico personal según la reivindicación 17, caracterizado porque dicha interpretación de los segundos datos recibidos incluye identificar si dicha parte de los segundos datos adicionales recibidos se ha modificado o no con dicho material de clave derivada y el componente léxico personal realiza las siguientes etapas:

g1) si dicha parte de los segundos datos se ha modificado al menos con dicha parte del material de clave derivada, el componente léxico mantiene al menos una porción dada del material de clave derivada manteniéndola oculta en el componente léxico;

g2) si dicha parte de los segundos datos no se ha modificado, el componente léxico transmite al terminal dicha porción dada del material de clave derivada.

28.- El componente léxico personal según la reivindicación 27, caracterizado porque el componente léxico realiza un nuevo cálculo de dicha parte de los segundos datos sobre la base de dichos datos aleatorios (RAND) recibidos y sobre la base de la clave secreta (K) y mantiene una porción dada de material de clave derivada dentro del componente léxico manteniéndola oculta en el componente léxico en caso de que dicha parte recibida de los segundos datos no corresponda ni a la parte nuevamente calculada de los segundos datos, ni a dicha parte nuevamente calculada modificada con material de clave derivada.

29.- El componente léxico personal según cualquiera de las reivindicaciones 17 a 28, caracterizado porque el componente léxico personal envía a través del terminal una respuesta (RES) al servidor de autenticación y el servidor de autenticación autentica el componente léxico por medio de dicha respuesta, y en eso una vez que el servidor de autenticación y el servidor de autenticación se han autenticados mutuamente, el componente léxico

personal deriva una clave interna (KsNAFint) y una clave externa (KsNAFext) de dicha parte del material de clave derivada (Ck, Ik), siendo utilizada dicha clave interna (KsNAFint) para establecer un canal seguro entre el componente léxico personal y un servidor remoto a través del terminal pero oculto al terminal, y siendo utilizada dicha clave externa (KsNAFext) para establecer un canal seguro entre el terminal y un servidor remoto.

30.- Un servidor de autenticación en una red de comunicación, que autentica terminales, cada una de las cuales aloja un componente léxico personal, realizando dicho servidor de autenticación las siguientes etapas:

a. recibir de un servidor seguro datos aleatorios (RAND) de material de clave derivada (Ck, Ik) producido sobre la base de dichos datos aleatorios (RAND) y primeros datos (AUTN, XRES, MAC, SQN, Ak, AMF);

b. generar segundos datos (MAC*, SQN*) modificando al menos parte de dichos primeros datos por medio al menos de parte de dicho material de clave derivada (Ck, Ik),

c. enviar dichos segundos datos y dichos datos aleatorios (RAND) a través de un terminal al componente léxico personal alojado en un terminal.

d. autenticar el componente léxico personal por medio de dicha respuesta recibida del componente léxico personal a través del terminal, y

e. si el servidor de autenticación y el componente léxico personal se autentican mutuamente, derivar una clave interna (KsNAFint) y una clave externa (KsNAFext) desde dicha parte del material de clave derivada (Ck, Ik), siendo utilizada dicha clave interna (KsNAFint) para establecer un canal seguro entre el componente léxico personal y un servidor remoto a través del terminal pero oculto al terminal, y siento utilizada dicha clave externa (KsNAFext) para establecer un canal seguro entre el terminal y un servidor remoto.

31.- Un programa informático para un servidor de autenticación en una red de comunicación, cuyo servidor autentica terminales en la red, cada uno de los cuales aloja un componente léxico personal, incluyendo dicho programa informático instrucciones de programa para ejecutar las siguientes etapas:

a. recibir de un servidor seguro datos aleatorios (RAND) de material de clave derivada (Ck, Ik) producido sobre la base de dichos datos aleatorios (RAND) y primeros datos (AUTN, XRES, MAC, SQN, Ak, AMF);

b. generar segundos datos (MAC*, SQN*) modificando al menos parte de dichos primeros datos por medio de al menos parte de dicho material de clave derivada (Ck, Ik),

c. enviar dichos segundos datos y dichos datos aleatorios (RAND) a través de un terminal al componente léxico personal alojado en el terminal.

d. autenticar el componente léxico personal por medio de dicha respuesta recibida del componente léxico personal a través del terminal, y

e. si el servidor de autenticación y el componente léxico personal se autentican mutuamente, derivar una clave interna (KsNAFint) y una clave externa (KsNAFext) desde dicha parte del material de clave derivada (Ck, Ik), siendo utilizada dicha clave interna (KsNAFint) para establecer un canal seguro entre el componente léxico personal y un servidor remoto a través del terminal pero oculto al terminal, y siento utilizada dicha clave externa (KsNAFext) para establecer un canal seguro entre el terminal y un servidor remoto.

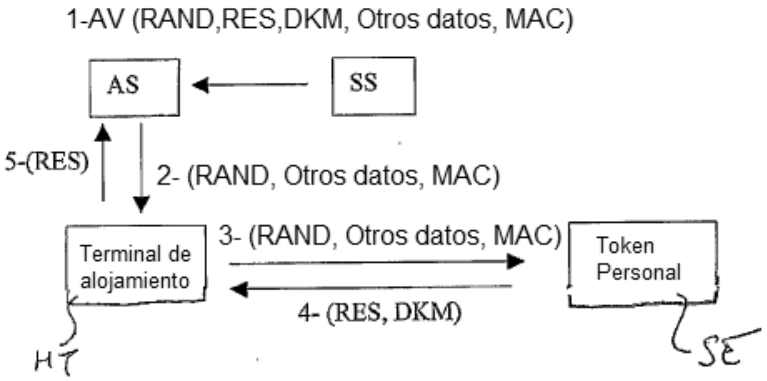
1-AV (RAND,RES,DKM, Otros datos, MAC)
AS
SS
5-(RES)
2- (RAND, Otros datos, MAC)
Terminal de alojamiento
3- (RAND, Otros datos, MAC)
4- (RES, DKM)
Token Personal
HT
SE

Fig. 1

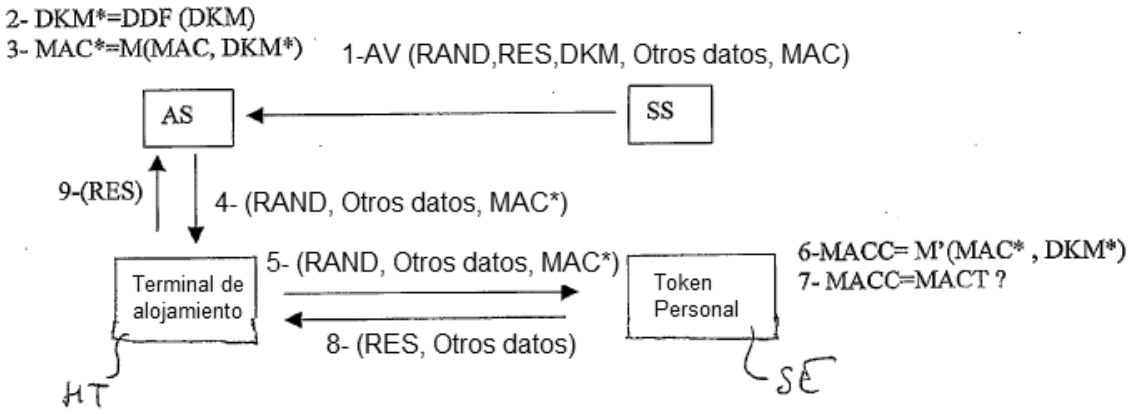
2- DKM*=DDF (DKM)
3- MAC*=M(MAC, DKM*)
1-AV (RAND,RES,DKM, Otros datos, MAC)
AS
SS
9-(RES)
4- (RAND, Otros datos, MAC*)
Terminal de alojamiento
5- (RAND, Otros datos, MAC*)
8- (RES, Otros datos)
Token Personal
6-MACC= M'(MAC* , DKM*)
7- MACC=MACT ?
HT
SE

Fig. 2