(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 698 449**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.10.2008 PCT/CN2008/072795**

(87) Fecha y número de publicación internacional: **07.05.2009 WO09056049**

(96) Fecha de presentación y número de la solicitud europea: **23.10.2008 E 08844910 (3)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 2214429**

(54) Título: **Método y sistema de identificador bidireccional de entidad basado en una tercera parte de confianza**

(30) Prioridad:

23.10.2007 CN 200710018920

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.02.2019

(73) Titular/es:

CHINA IWNCOMM CO., LTD. (100.0%)
A201 Qin Feng Ge Xi'an Software Park No. 68 Ke Ji 2nd Road Xi'an Hi-Tech Industrial Development Zone
Xi'an, Shaanxi 710075, CN

(72) Inventor/es:

TIE, MANXIA;
CAO, JUN;
LAI, XIAOLONG;
PANG, LIAOJUN y
HUANG, ZHENHAI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y sistema de identificador bidireccional de entidad basado en una tercera parte de confianza

Esta solicitud reivindica la prioridad a la solicitud de patente china n.º 200710018920.6, presentada ante la Oficina de Patentes de China el 23 de octubre de 2007 y titulada "MÉTODO Y SISTEMA PARA LA AUTENTIFICACIÓN MUTUA DE LAS ENTIDADES BASADAS EN UNA TERCERA PARTE DE CONFIANZA".

Campo de la invención

La presente invención se refiere al campo de las comunicaciones y, en particular, a un método para la autentificación mutua de entidades basándose en una tercera parte de confianza y a un sistema del mismo.

Antecedentes de la invención

En la actualidad, la autentificación mutua se implementa normalmente entre un usuario y un punto de acceso a la red a través de una red de comunicación para garantizar el acceso de un usuario válido a una red válida. Los métodos de autentificación de entidades que utilizan una técnica criptográfica asimétrica se pueden clasificar en dos tipos: autentificación unilateral y autentificación mutua. En particular, la unicidad/puntualidad de la autentificación se controla mediante la generación y la verificación de parámetros de variante de tiempo, tales como sellos de tiempo, números de secuencia o números aleatorios. Si los sellos de tiempo o los números de secuencia se utilizan como parámetros de variante de tiempo, la autentificación mutua entre entidades se puede completar mediante la autentificación de dos pasos; o si se usan números aleatorios como parámetros de variante de tiempo, la autentificación mutua entre entidades se puede completar mediante una autentificación de tres pasos o dos autentificaciones paralelas.

Antes o durante la operación del mecanismo de autentificación, un verificador estará provisto de una clave pública válida de un demandante, de lo contrario la autentificación podría estar en peligro o fallar. Una autentificación mutua de tres pasos se describe aquí como un ejemplo.

Haciendo referencia a la figura 1, el sistema de autentificación incluye dos entidades de autentificación A y B. La entidad de autentificación A transmite un contador ContadorAB=$R_A\|R_B\|B\|Texto3\|sS_A(R_A\|R_B\|B\|Texto2)$ a la entidad de autentificación B, y la autentificación de la entidad B transmite un contador ContadorBA=$R_B\|R_A\|A\|Texto5\|sS_B(R_B\|R_A\|A\|Texto4)$ a la entidad de autentificación a, donde sS_X indica una firma de una entidad X, R_X indica un número aleatorio generado por la entidad X, $Cert_X$ indica un certificado de la entidad X, y Texto2, Texto3, Texto4 y Texto5 indican campos de texto opcionales, y X indica un identificador distintivo de la entidad de autentificación, aquí A o B.

Un proceso de operación el mecanismo de autentificación de tres pasos se describe en detalle a continuación:

1) La entidad B transmite un número aleatorio R_B y un campo de texto opcional Texto1 a la entidad A;

2) La entidad A transmite un contador ContadorAB y un campo de certificado opcional $Cert_A$ a la entidad B;

3) La entidad B realiza las siguientes etapas al recibir el mensaje transmitido desde la entidad A:

3.1) Garantizar la obtención de una clave pública válida de la entidad A, ya sea mediante la verificación del certificado de la entidad A o por algún otro medio; y

3.2) Verificar la firma de la entidad A contenida en el contador ContadorAB en la etapa 2), comprobando la exactitud del identificador distintivo de la entidad B, y verificando que el número aleatorio R_B transmitido en la etapa 1) es coherente con el número aleatorio R_B contenido en el contador ContadorAB, de modo que la entidad A sea autentificada por la entidad B;

4) La entidad B transmite el contador ContadorBA y un campo de certificado opcional $Cert_B$ a la entidad A; y

5) La entidad A realiza las siguientes etapas al recibir el mensaje, incluido el contador ContadorBA transmitido desde la entidad B:

5.1) Garantizar la obtención de una clave pública válida para la entidad B, ya sea mediante la verificación del certificado de la entidad B o por algún otro medio; y

5.2) Verificar la firma de la entidad B contenida en el contador ContadorBA en la etapa 4), verificando la corrección del identificador distintivo de la entidad A, y comprobando que el número aleatorio R_A transmitido en la etapa 2) sea coherente con el número aleatorio R_A contenido en el contador ContadorBA y que el número aleatorio R_B recibido en la etapa 1) es coherente con el número aleatorio R_B contenido en el contador

ContadorBA, de modo que la entidad A autentifica la entidad B.

Como puede ser evidente, la operación con éxito del mecanismo de autentificación de tres pasos se garantiza con la condición de que la entidad A y la entidad B poseen respectivamente las claves públicas válidas entre sí, pero el protocolo no implica cómo obtener las claves públicas válidas y la validez de las mismas. Sin embargo, esta condición de garantía no se puede satisfacer en muchos escenarios de aplicaciones en la actualidad. Por ejemplo, una función de control de acceso de usuario se realiza normalmente mediante el mecanismo de autentificación de la entidad a través de una red de comunicación, y por lo tanto se prohíbe el acceso de un usuario a la red antes de una operación exitosa del mecanismo de autentificación, y por lo tanto es imposible o difícil para el usuario acceder a una autoridad de certificación, e incluso es imposible obtener la validez de la clave pública de una entidad opuesta, es decir, un punto de acceso a la red, antes de la autentificación.

JESSE WALKER describe una versión del estándar "IEEE P802.11 LAN inalámbricas", en el documento JTC1 SC6 doc 6N12687 de 12 de diciembre de 2004, páginas 1-74, según lo remitido por la Secretaría de la ISO/CEI JTC1/SC6.

El documento US 5.491.750 describe un método para autentificar socios de comunicación utilizando flujos de comunicación que se pasan a través de un canal de comunicación inseguro. Se proporciona un intermediario de confianza que es capaz de comunicarse con los socios de comunicación a través del canal de comunicación inseguro. Los intermediarios de confianza y los socios de comunicación intercambian pruebas de autentificación entre sí en una pluralidad de flujos de comunicación.

El documento de normalización "ISO/IEC 9798, Tecnología de información - Técnicas de seguridad - Autentificación de la entidad", "Parte 3: Mecanismos que utilizan técnicas de firma digital", de 15-10-1998, páginas 1-6, especifican mecanismos de autentificación de entidad que utilizan firmas digitales basadas en técnicas asimétricas.

ROBERT Zuccherato define en "ISO/IEC 9798-3 Mecanismo de autentificación SASL", draft-Zuccherato-9798-3-sasl-03.txt", 20010501, n.º 3, 1 de mayo de 2001, un mecanismo de autentificación basado en ISO/IEC 9798-3 [ISO3] y FIPS PUB 196 [FIPS]. Este mecanismo solo proporciona autentificación utilizando certificados X.509.

Sumario de la invención

La invención es de acuerdo con las reivindicaciones adjuntas. Para abordar el problema técnico en la técnica anterior, se propone un método y un sistema para la autentificación mutua de entidades basadas en una tercera parte de confianza, de modo que las entidades no autentificadas puedan autentificarse exitosamente sin el conocimiento requerido de una clave pública válida de una entidad de comunicación opuesta antes de la autentificación.

Una realización proporciona un método para la autentificación mutua de las entidades basándose en una tercera parte de confianza, que incluye:

etapa 1). transmitir un primer mensaje de una primera entidad a una segunda entidad, incluyendo el primer mensaje un primer parámetro de variante de tiempo $R1_A$ generado por la primera entidad, el identificador ID_A de la primera entidad y un primer campo de texto opcional Texto1

etapa 2). transmitir un segundo mensaje de la segunda entidad a la primera entidad al recibir el primer mensaje, incluyendo el segundo mensaje un contador ContadorBA transmitido desde la segunda entidad a la primera entidad, el identificador ID_B de la segunda entidad y un segundo campo de texto opcional Texto2;

etapa 3). transmitir un tercer mensaje desde la primera entidad a una tercera entidad al recibir el segundo mensaje, incluyendo el tercer mensaje un segundo parámetro de variante de tiempo $R2_A$ generado por la primera entidad, un parámetro de variante de tiempo R_B generado por la segunda entidad, el identificador El ID_A de la primera entidad, el identificador ID_B de la segunda entidad y un tercer campo de texto opcional Texto3;

etapa 4). verificar por una tercera entidad al recibir el tercer mensaje si la primera entidad y la segunda entidad son legales, y realizar un proceso de ajuste previo en respuesta a un resultado de verificación;

etapa 5). transmitir un cuarto mensaje desde la tercera entidad a la primera entidad, incluyendo el cuarto mensaje un contador ContadorTA transmitido desde la tercera entidad a la primera entidad y un cuarto campo de texto de opción Texto4;

etapa 6). verificar el cuarto mensaje de la primera entidad al recibir el cuarto mensaje, para completar la autentificación de la segunda entidad después de que la primera entidad verifique el cuarto mensaje;

etapa 7). transmitir un quinto mensaje desde la primera entidad a la segunda entidad, incluyendo el quinto mensaje el contador ContadorTA transmitido desde la tercera entidad a la primera entidad, un contador

ContadorAB transmitido desde la primera entidad a la segunda entidad y un quinto campo de texto opcional Texto5 o incluyendo un segundo subcontador ContadorTA2 transmitido desde la tercera entidad a la primera entidad, un contador ContadorAB transmitido desde la primera entidad a la segunda entidad y un quinto campo de texto opcional Texto5; y

etapa 8). verificar el quinto mensaje por la segunda entidad al recibir el quinto mensaje, para completar la autentificación de la primera entidad después de que la segunda entidad verifique el quinto mensaje.

Preferiblemente, la etapa 4) de verificar si la primera entidad y la segunda entidad son legales y realizar el proceso de ajuste previo en respuesta al resultado de la verificación incluye: si el ID_A y el ID_B en el tercer mensaje son certificados, verificando el certificado de la primera entidad y el certificado de la segunda entidad para su validez, y si el certificado de la primera entidad y/o el certificado de la segunda entidad no es válido, descartar el tercer mensaje y finalizar el flujo de autentificación, o devolver el cuarto mensaje a la primera entidad e ir a la etapa 5); o si el certificado de la primera entidad y el certificado de la segunda entidad son válidos, devolver el cuarto mensaje a la primera entidad y pasar a la etapa 5).

Preferiblemente, la etapa 4) de verificar si la primera entidad y la segunda entidad son legales y realizar el proceso de ajuste previo en respuesta al resultado de la verificación incluye: si el ID_A y el ID_B en el tercer mensaje están distinguiendo identificadores, verificar la validez de una clave pública de la primera entidad y una clave pública de la segunda entidad, y si la clave pública de la primera entidad y/o la clave pública de la segunda entidad no es válida, descartar el tercer mensaje y finalizar el flujo de autentificación, o, devolver el cuarto mensaje a la primera entidad; o si la clave pública de la primera entidad y la clave pública de la segunda entidad son válidas, devolver el cuarto mensaje a la primera entidad.

Preferiblemente, la etapa 6) de verificación del cuarto mensaje por la primera entidad incluye: 601. verificar una firma de la tercera entidad contenida en el ContadorTA o un primer contador ContadorTA 1 transmitido desde la tercera entidad a la primera entidad y si $R2_A$ en el tercer mensaje es coherente con $R2_A$ en el ContadorTA o el ContadorTA1, y si se pasa la verificación, obtener el resultado de verificar la segunda entidad, determinar si la segunda entidad es legal y si la segunda entidad es legal, ir a la etapa 602; si la segunda entidad es ilegal, finalizar el flujo de autentificación o ir a la etapa 7); y 602. obtener una clave pública de la segunda entidad, verificar una firma de la segunda entidad contenida en el ContadorBA en el segundo mensaje y si el $R1_A$ en el primer mensaje es coherente con $R1_A$ en el ContadorAB, y si la verificación se ha pasado, ir a la etapa 7), de modo que la segunda entidad sea autentificada por la primera entidad.

Preferiblemente, la etapa 8) de verificación del quinto mensaje por la segunda entidad incluye: 801. verificar una firma de la tercera entidad contenida en el ContadorTA o el ContadorTA2 y si R_B en el segundo mensaje es coherente con R_B en el ContadorTA o el ContadorTA2, y si se pasa la verificación, obtener un resultado de la verificación de la primera entidad, que determina si la primera entidad es válida y si la primera entidad es válida, ir a la etapa 802; si la primera entidad no es válida, finalizar el flujo de autentificación; y 802. obtener una clave pública de la primera entidad, verificar que la firma de la primera entidad contenida en el ContadorAB y el R_B en el segundo mensaje es coherente con el R_B en el ContadorAB, y si se pasa la verificación, la segunda entidad completa la autentificación de la primera entidad.

Preferiblemente, el $R2_A$ en el tercer mensaje puede ser el mismo que el $R1_A$ en el primer mensaje.

Preferiblemente, los parámetros variantes en el tiempo pueden ser números aleatorios, etiquetas de tiempo o números de serie.

Preferiblemente, la etapa 1) es opcional si los parámetros variantes en el tiempo son números aleatorios o etiquetas de tiempo.

Otra realización de la presente invención proporciona un sistema para la autentificación mutua de entidades basándose en una tercera parte de confianza, que incluye: una primera entidad, adaptada para transmitir un primer mensaje a una segunda entidad, para transmitir un tercer mensaje a una tercera entidad tras la recepción de un segundo mensaje transmitido desde la segunda entidad, para verificar un cuarto mensaje tras la recepción del cuarto mensaje transmitido desde la tercera entidad, y para transmitir un quinto mensaje a la segunda entidad después de la verificación; estando la segunda entidad adaptada para recibir el primer mensaje transmitido desde la primera entidad, para transmitir el segundo mensaje a la primera entidad, y para verificar el quinto mensaje tras la recepción del quinto mensaje transmitido desde la primera entidad; y estando la tercera entidad adaptada para recibir el tercer mensaje transmitido desde la primera entidad, para verificar si la primera entidad y la segunda entidad son legales, para realizar un proceso de ajuste previo en respuesta a un resultado de verificación, y para transmitir el cuarto mensaje a la primera entidad después del proceso.

Una realización de la invención proporciona un sistema para la autentificación mutua de entidades basándose en una tercera parte de confianza, que incluye: una primera entidad adaptada para transmitir un primer mensaje a una segunda entidad, para transmitir un tercer mensaje a una tercera entidad al recibir un segundo mensaje transmitido

desde la segunda entidad, para verificar un cuarto mensaje tras la recepción del cuarto mensaje transmitido desde la tercera entidad, y para transmitir un quinto mensaje a la segunda entidad después de la autentificación; estando la segunda entidad adaptada para recibir el primer mensaje transmitido desde la primera entidad, para transmitir el segundo mensaje a la primera entidad, y para verificar el quinto mensaje tras la recepción del quinto mensaje transmitido desde la primera entidad; y estando la tercera entidad adaptada para recibir el tercer mensaje transmitido desde la primera entidad, para verificar la legalidad de la primera entidad y la segunda entidad, para realizar un proceso de ajuste previo en respuesta a un resultado de verificación, y para transmitir el cuarto mensaje a la primera entidad después del proceso.

Como puede ser evidente a partir de las realizaciones previamente descritas de la invención, una arquitectura de triple entidad se puede adoptar para que las entidades de autentificación recuperen una clave pública o un certificado de una tercera entidad antes de la autentificación y recuperar un certificado de usuario expedido a la misma para su uso desde la tercera entidad o enviar su propia clave pública a la tercera entidad para su custodia sin necesidad de conocer previamente una clave pública válida de una entidad de autentificación opuesta. Durante la operación de un protocolo, la clave pública de una de las entidades de autentificación y su validez se pueden pasar automáticamente a la entidad de autentificación opuesta a través de la recuperación y verificación por parte de la entidad de terceros. En comparación con los mecanismos de autentificación tradicionales, las realizaciones de la invención definen un mecanismo de recuperación y autentificación en línea de claves públicas para permitir así la gestión centralizada de las claves públicas, simplificar la condición de operar el protocolo y lograr una buena viabilidad y facilidad de uso en una aplicación práctica.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático de un mecanismo de autentificación de tres pasos en la técnica anterior; y

La figura 2 es un diagrama esquemático de un método de autentificación mutua según la invención.

Descripción detallada de la invención

Se hace referencia a la figura 2, que ilustra un diagrama esquemático de un método de autentificación mutua de acuerdo con la invención. Una realización de la invención implica tres entidades, es decir, dos entidades de autentificación A y B y una entidad de tercera parte de confianza (TP) que es una tercera parte de confianza de las entidades de autentificación A y B, donde $Válido_X$ indica la validez de un certificado $Cert_X$, $ClavePública_X$ es una clave pública de una entidad X, ID_X es un identificador de la entidad X, que se representa con $Cert_X$ o X, Pub_X indica un resultado de verificar la entidad X y está compuesto del certificado $Cert_X$ y la validez $Válido_X$ del mismo o compuesto por la entidad X y la clave pública $ClavePública_X$ del mismo, y X es un identificador distintivo de la entidad de autentificación, en la presente realización, A o B.

En la presente realización, los respectivos contadores se definen como sigue:

ContadorBA=$R1_A\|R_B\|ID_A\|sS_B(R1_A\|R_B\|ID_A\|Texto2)$: un contador transmitido a la entidad de autentificación A desde la entidad de autentificación B, donde $R1_A$ es un primer número aleatorio generado por la entidad de autentificación A;

ContadorAB = $sS_A(R_B\|R1_A\|ID_B\|Texto5\|ContadorTA)$: un contador transmitido a la entidad de autentificación B desde la autentificación A;

ContadorTA=$R2_A\|R_B\|Pub_A\|Pub_B\|sS_{TP}(R2_A\|R_B\|Pub_A\|Pub_B\|Texto4)$: un contador transmitido a la entidad de autentificación A desde la tercera parte de confianza, donde $R2_A$ es un segundo número aleatorio generado por la entidad autentificadora A.

Alternativamente, se pueden definir como sigue:

$$ContadorTA=ContadorTA1\|ContadorTA2$$

$$ContadorTA1=R2_A\|Pub_B\|Texto6\|sS_{TP}(R2_A\|Pub_B\|Texto6)$$

$$ContadorTA2=R_B\|Pub_A\|Texto7\|sS_{TP}(R_B\|Pub_A\|Texto7)$$

Un flujo específico del método es el siguiente:

1) La entidad de autentificación A transmite a la entidad de autentificación B un mensaje 1 que incluye el primer número aleatorio $R1_A$ generado por la entidad de autentificación A, el identificador ID_A de la entidad de autentificación A y un campo de texto opcional Texto1.

2) Al recibir el mensaje 1, la entidad de autentificación B transmite a la entidad de autentificación A un mensaje 2 que incluye el contador ContadorBA transmitido desde la entidad de autentificación B a la entidad de autentificación A, el identificador ID_B de la entidad de autentificación B y un campo de texto opcional Texto2.

3) Al recibir el mensaje 2, la entidad de autentificación A transmite a la entidad de tercera parte de confianza un mensaje 3 que incluye el segundo número aleatorio $R2_A$ generado por la entidad de autentificación A, un número aleatorio R_B generado por la entidad de autentificación B, el identificador ID_A de la entidad de autentificación A, el identificador ID_B de la entidad de autentificación B y un campo de texto opcional Texto3.

4) La entidad de tercera parte de confianza verifica la entidad de autentificación A y la entidad de autentificación para determinar la legalidad al recibir el mensaje 3.
En particular, si los identificadores de la entidad de autentificación A y la entidad de autentificación B en el mensaje 3 son certificados, se verifica la validez del certificado de la entidad de autentificación A y el certificado de la entidad de autentificación B; y si el certificado de la entidad de autentificación A y/o el certificado de la entidad de autentificación B no es válido, el mensaje 3 se descarta directamente y el flujo de autentificación finaliza, o bien, se devuelve un mensaje 4 a la entidad de autentificación A y el flujo va a la etapa 5); y si el certificado de la entidad de autentificación A y el certificado de la entidad de autentificación B son válidos, el mensaje 4 se devuelve a la entidad de autentificación A y el flujo va a la etapa 5).
Si los identificadores de la entidad de autentificación A y la entidad de autentificación B en el mensaje 3 son identificadores distintivos, la clave pública de la entidad de autentificación A y la clave pública de la entidad de autentificación B se verifican para su validez, y si la clave pública de la entidad de autentificación A y/o la clave pública de la entidad de autentificación B no es válida, el mensaje 3 se descarta directamente y el flujo de autentificación finaliza, o el mensaje 4 se devuelve a la entidad de autentificación A y el flujo va a la etapa 5) ; y si la clave pública de la entidad de autentificación A y la clave pública de la entidad de autentificación B son válidas, el mensaje 4 se devuelve a la entidad de autentificación A y el flujo va a la etapa 5).

5) La entidad de tercera parte de confianza transmite a la entidad de autentificación A el mensaje 4 que incluye el contador ContadorTA transmitido desde la entidad de tercera parte de confianza a la entidad de autentificación A y un campo de texto opcional Texto4.

6) La entidad de autentificación A verifica el mensaje 4 al recibir el mensaje 4.
En particular, este proceso de verificación incluye:

6.1) Verificar una firma de la entidad de tercera parte de confianza contenida en el contador ContadorTA o el contador ContadorTA1 y si el segundo número aleatorio $R2_A$ generado por la entidad de autentificación A en el mensaje 3 es coherente con $R2_A$ en el contador ContadorTA o el contador ContadorTA1; si se pasa la verificación, se va a la etapa 6.2);

6.2) Obtener un Pub_B resultante de la verificación de la entidad de autentificación B, que determina si la entidad de autentificación B es legal y si la entidad de autentificación B es legal, ir a la etapa 6.3); de lo contrario, finalizar el flujo de autentificación o ir a la etapa 7); y

6.3) Obtener la clave pública de la entidad de autentificación B, verificar una firma de la entidad de autentificación B contenida en el contador ContadorBA en el mensaje 2 y si el número aleatorio $R1_A$ generado por la entidad de autentificación A en el mensaje 1 es coherente con $R1_A$ en el contador ContadorBA; si se pasa la verificación, ir a la etapa 7), donde la primera entidad completa la autentificación de la segunda entidad.

7) La entidad de autentificación A transmite a la entidad de autentificación B un mensaje 5 que incluye el contador ContadorTA, el contador ContadorAB y un campo de texto opcional Texto5 o que incluye el contador ContadorTA2, el contador ContadorAB y un campo de texto opcional Texto5.

8) La entidad de autentificación B verifica el mensaje 5 al recibir el mensaje 5.
En particular, este proceso de verificación incluye:

8.1) Verificar una firma de la tercera parte de confianza contenida en el contador ContadorTA o el contador ContadorTA2 y si el R_B generado por la entidad de autentificación B en el mensaje 2 es coherente con el R_B en el contador ContadorTA o el contador ContadorTA2; si se pasa la verificación, ir a la etapa 8.2);

8.2) Obtener un resultado Pub_A de verificar la entidad de autentificación A, determinar si la entidad de autentificación A es legal y si la entidad de autentificación A es legal, ir a la etapa 8.3); si la entidad de autentificación A es ilegal, finalizar el flujo de autentificación; y

8.3) Obtener la clave pública de la entidad de autentificación A, verificar una firma de la entidad de autentificación A contenida en el contador ContadorAB y si R_B en el mensaje 2 es coherente con R_B en el contador ContadorAB, y si se pasa la verificación, la segunda entidad ha completado la autentificación de la

primera entidad.

Se observará que los parámetros variantes en el tiempo son números aleatorios en la realización anterior. Alternativamente, los sellos de tiempo o los números de secuencia se pueden usar como parámetros de la variante de tiempo, y en este caso, el mensaje 1 es un mensaje opcional, es decir, la etapa 1) se puede omitir.

En correspondencia con un método para la autentificación mutua de las entidades basándose en una tercera parte de confianza en la realización anterior de la invención, una realización de la invención proporciona además un sistema para la autentificación mutua de entidades basándose en una tercera parte de confianza, que incluye una entidad A, una entidad B y una entidad de tercera parte de confianza, en la que cualquiera de las entidades A y B conectadas entre sí puede estar conectada con la entidad de tercera parte de confianza. La entidad de tercera parte de confianza puede ser una entidad de servicio de autentificación ya existente o recientemente agregada al sistema. Por ejemplo, la entidad de tercera parte de confianza puede ser un servidor de autentificación ya existente o recientemente agregado al sistema en una aplicación para un usuario y un punto de acceso a la red.

REIVINDICACIONES

1. Un método para la autentificación mutua de entidades (A, B) basada en una tercera entidad de confianza (TP), que comprende:

etapa 1). transmitir un primer mensaje desde una primera entidad (A) a una segunda entidad (B), comprendiendo el primer mensaje un primer parámetro de variante de tiempo $R1_A$ generado por la primera entidad (A), un identificador ID_A de la primera entidad (A) y un primer campo de texto opcional Texto1;
etapa 2). transmitir un segundo mensaje desde la segunda entidad (B) a la primera entidad (A) al recibir el primer mensaje, comprendiendo el segundo mensaje un contador ContadorBA transmitido desde la segunda entidad (B) a la primera entidad (A), un identificador ID_B de la segunda entidad (B) y un segundo campo de texto opcional Texto2;
etapa 3). transmitir un tercer mensaje desde la primera entidad (A) a la tercera entidad de confianza (TP) al recibir el segundo mensaje, comprendiendo el tercer mensaje un segundo parámetro de variante de tiempo $R2_A$ generado por la primera entidad (A), un parámetro de variante de tiempo R_B generado por la segunda entidad (B) e incluido en el contador ContadorBA, el identificador ID_A de la primera entidad (A), el identificador ID_B de la segunda entidad (B) y un tercer campo de texto opcional Texto3;
etapa 4). verificar por la tercera entidad de confianza (TP) al recibir el tercer mensaje si la primera entidad (A) y la segunda entidad (B) son legales de acuerdo con la información transportada en el tercer mensaje, y realizar un proceso de ajuste previo en respuesta a un resultado de verificación;
etapa 5). transmitir un cuarto mensaje de la tercera entidad de confianza (TP) a la primera entidad (A), comprendiendo el cuarto mensaje un contador ContadorTA y un cuarto campo de texto opcional Texto4, en donde el contador ContadorTA comprende una clave pública de la segunda entidad (B);
etapa 6). verificar el cuarto mensaje de la primera entidad (A) al recibir el cuarto mensaje, para completar la autentificación de la segunda entidad (B) después de que la primera entidad (A) verifique el cuarto mensaje;
etapa 7). transmitir un quinto mensaje desde la primera entidad (A) a la segunda entidad (B), comprendiendo el quinto mensaje el contador ContadorTA transmitido desde la tercera entidad de confianza (TP) a la primera entidad (A), un contador ContadorAB y un quinto campo de texto opcional Texto5 o que incluye un contador ContadorTA2 transmitido desde la tercera entidad (TP) a la primera entidad (A), el contador ContadorAB y el quinto campo de texto opcional Texto5, en donde cada uno del contador ContadorTA y el contador ContadorTA2 comprende una clave pública de la primera entidad (A) y en donde el contador ContadorTA2 es un subcontador del contador ContadorTA; y
etapa 8). verificar el quinto mensaje por la segunda entidad (B) al recibir el quinto mensaje, para completar la autentificación de la primera entidad (A) después de que la segunda entidad (B) verifique el quinto mensaje;

en el que la etapa 6) de verificar el cuarto mensaje por la primera entidad (A) comprende:

601. verificar una firma de la tercera entidad de confianza (TP) contenida en el contador ContadorTA o en un contador ContadorTA1 transmitido desde la tercera entidad (TP) a la primera entidad (A) y si $R2_A$ en el tercer mensaje es coherente con $R2_A$ en el contador ContadorTA o en el contador ContadorTA1, en donde el contador ContadorTA1 es un subcontador del contador ContadorTA, y si se pasa la verificación se obtiene un resultado de la verificación de la segunda entidad (B), que determina si la segunda entidad (B) es legal, y si la segunda entidad (B) es legal, ir a la etapa 602; si la segunda entidad (B) es ilegal, finalizar el flujo de autentificación o ir a la etapa 7); y
602. obtener la clave pública de la segunda entidad (B), verificar una firma de la segunda entidad (B) contenida en el contador ContadorBA en el segundo mensaje y si $R1_A$ en el primer mensaje es coherente con $R1_A$ en el contador ContadorAB, y si se pasa la verificación, ir a la etapa 7), de modo que la segunda entidad (A) autentifique la segunda entidad (B);

en el que la etapa 8) de verificar el quinto mensaje por la segunda entidad (B) comprende:

801. verificar una firma de la tercera entidad de confianza (TP) contenida en el contador ContadorTA o en el contador ContadorTA2 y si R_B en el segundo mensaje es coherente con R_B en el contador ContadorTA o en el contador ContadorTA2, y si se pasa la verificación, obtener el resultado de verificar la primera entidad (A), determinar si la primera entidad (A) es válida y si la primera entidad (A) es válida, ir a la etapa 802; si la primera entidad (A) no es válida, finalizar el flujo de autentificación; y
802. obtener la clave pública de la primera entidad (A), verificar una firma de la primera entidad (A) contenida en el contador ContadorAB y si el R_B en el segundo mensaje es coherente con el R_B en el contador ContadorAB, y si se pasa la verificación, la segunda entidad (B) completa la autentificación de la primera entidad (A).

2. El método según la reivindicación 1, en el que la etapa 4) de verificar si la primera entidad (A) y la segunda entidad (B) son legales y realizar el proceso de ajuste previo en respuesta al resultado de la verificación comprende:
si el ID_A y el ID_B en el tercer mensaje son certificados, verificar la validez del certificado de la primera entidad (A) y del certificado de la segunda entidad (B), y si el certificado de la primera entidad (A) y/o el certificado de la segunda entidad (B) no son válidos, descartar el tercer mensaje y finalizar el flujo de autentificación; o si el certificado de la primera entidad (A) y el certificado de la segunda entidad (B) son válidos, devolver el cuarto mensaje a la primera

entidad (A) e ir a la etapa 5).

3. El método según la reivindicación 1, en el que la etapa 4) de verificar si la primera entidad (A) y la segunda entidad (B) son legales y realizar el proceso de ajuste previo en respuesta al resultado de la verificación comprende: si el ID_A y el ID_B en el tercer mensaje son identificadores distintivos, verificar la validez de una clave pública de la primera entidad (A) y una clave pública de la segunda entidad (B), y si la clave pública de la primera entidad (A) y/o la clave pública de la segunda entidad (B) no son válidas, descartar el tercer mensaje y finalizar el flujo de autentificación; o si la clave pública de la primera entidad (A) y la clave pública de la segunda entidad (B) son válidas, devolver el cuarto mensaje a la primera entidad (A) e ir a la etapa 5).

4. El método según la reivindicación 1, en el que el $R2_A$ en el tercer mensaje es el mismo que el $R1_A$ en el primer mensaje.

5. El método según la reivindicación 1, en el que los parámetros de variante de tiempo son números aleatorios, sellos de tiempo o números de secuencia.

6. Un sistema para la autentificación mutua de entidades (A, B) basada en una tercera entidad de confianza (TP), que comprende:

una primera entidad (A), adaptada para transmitir un primer mensaje a una segunda entidad, para transmitir un tercer mensaje a la tercera entidad de confianza (TP) al recibir un segundo mensaje transmitido desde la segunda entidad (B), para verificar un cuarto mensaje al recibir el cuarto mensaje transmitido desde la tercera entidad (TP), y para transmitir un quinto mensaje a la segunda entidad (B) después de la verificación; en donde el primer mensaje comprende un primer parámetro de variante de tiempo $R1_A$ generado por la primera entidad (A), un identificador ID_A de la primera entidad (A) y un primer campo de texto opcional Texto1; el tercer mensaje comprende un segundo parámetro de variante de tiempo $R2_A$ generado por la primera entidad (A), un parámetro de variante de tiempo R_B generado por la segunda entidad (B), el identificador ID_A de la primera entidad (A), un identificador ID_B de la segunda entidad (B) y un tercer campo de texto opcional Texto3; el cuarto mensaje comprende un contador ContadorTA y un cuarto campo de texto opcional Texto4, el contador ContadorTA comprende una clave pública de la segunda entidad (B); el quinto mensaje comprende el contador ContadorTA, un contador ContadorAB transmitido desde la primera entidad (A) a la segunda entidad (B) y un quinto campo de texto opcional Texto5, o un contador ContadorTA2 transmitido desde la tercera entidad de confianza (TP) a la primera la entidad (A) y el contador ContadorAB y el quinto campo de texto opcional Texto5, en donde cada uno del contador ContadorTA y el contador ContadorTA2 comprende una clave pública de la primera entidad (A), en donde el contador ContadorTA2 es un subcontador del contador ContadorTA;
la segunda entidad (B), adaptada para recibir el primer mensaje transmitido desde la primera entidad (A), para transmitir el segundo mensaje a la primera entidad (A), y para verificar el quinto mensaje tras la recepción del quinto mensaje transmitido desde la primera entidad (A), en donde el segundo mensaje comprende un contador ContadorBA transmitido desde la segunda entidad (B) a la primera entidad (A), el identificador ID_B de la segunda entidad (B) y un segundo campo de texto opcional Texto2, en donde el parámetro de variante de tiempo R_B está incluido en el contador ContadorBA; y
la tercera entidad de confianza (TP), adaptada para recibir el tercer mensaje transmitido desde la primera entidad (A), para verificar si la primera entidad (A) y la segunda entidad (B) son legales de acuerdo con la información transportada en el tercer mensaje, para realizar un proceso de ajuste previo en respuesta a un resultado de verificación y para transmitir el cuarto mensaje a la primera entidad (A) después del proceso;
en donde la primera entidad (A), adaptada para verificar el cuarto mensaje comprende: la primera entidad (A), adaptada para verificar una firma de la tercera entidad de confianza (TP) contenida en el contador ContadorTA o en un contador ContadorTA1 transmitido desde la tercera entidad de confianza (TP) a la primera entidad (A) y si el $R2_A$ en el tercer mensaje es coherente con el $R2_A$ en el contador ContadorTA o en el contador ContadorTA1, en donde el contador ContadorTA1 es un subcontador del contador ContadorTA, obtener un resultado de verificar la segunda entidad (B) si se pasa la verificación, determinar si la segunda entidad (B) es legal, obtener la clave pública de la segunda entidad (B) si la segunda entidad (B) es legal, verificar una firma de la segunda entidad (B) contenida en el contador ContadorBA en el segundo mensaje y si el $R1_A$ en el primer mensaje es coherente con $R1_A$ en el contador ContadorAB;
en donde la segunda entidad (B), adaptada para verificar el quinto mensaje, comprende: la segunda entidad (B), adaptada para verificar la firma de la tercera entidad de confianza (TP) contenida en el contador ContadorTA o en el contador ContadorTA2 y si R_B en el segundo mensaje es coherente con R_B en el contador ContadorTA o en el contador ContadorTA2, y si se pasa la verificación, obtener un resultado de la verificación de la primera entidad (A), determinar si la primera entidad (A) es válida, y si la primera entidad (A) es válida, obtener la clave pública de la primera entidad (A), verificar una firma de la primera entidad (A) contenida en el contador ContadorAB y si el R_B en el segundo mensaje es coherente con el R_B en el contador ContadorAB.

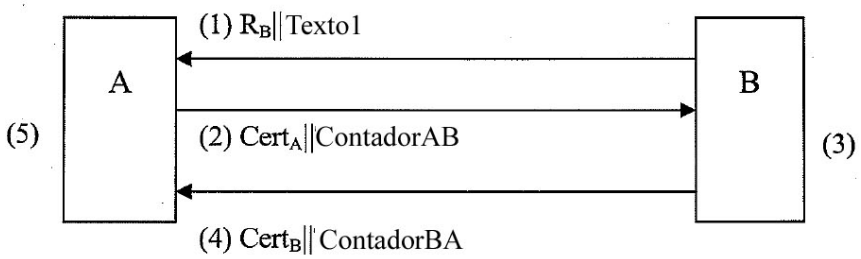
(1) R_B||Texto1
A
B
(5)
(2) $Cert_A$||ContadorAB
(3)
(4) $Cert_B$||ContadorBA

Fig.1

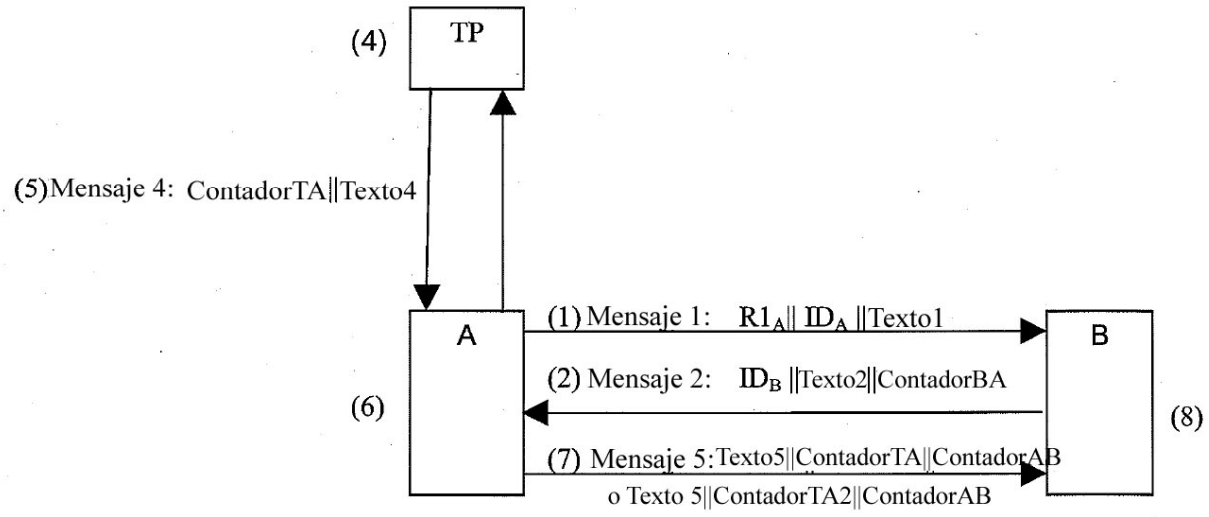
(4)
TP
(5)Mensaje 4: ContadorTA||Texto4
(1) Mensaje 1: $R1_A$|| ID_A ||Texto1
A
B
(2) Mensaje 2: ID_B ||Texto2||ContadorBA
(6)
(8)
(7) Mensaje 5:Texto5||ContadorTA||ContadorAB
o Texto 5||ContadorTA2||ContadorAB

Fig.2