(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 768 963**

(51) Int. CI.:

***H04L 9/32*** (2006.01)
***H04L 9/08*** (2006.01)
***H04L 9/00*** (2006.01)
***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.03.2015 PCT/CN2015/075285**

(87) Fecha y número de publicación internacional: **08.10.2015 WO15149658**

(96) Fecha de presentación y número de la solicitud europea: **27.03.2015 E 15772431 (1)**

(97) Fecha y número de publicación de la concesión europea: **20.11.2019 EP 3128696**

(54) Título: **Procedimiento y dispositivo de autenticación de entidad**

(30) Prioridad:

**31.03.2014 CN 201410126328**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**24.06.2020**

(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:

**HU, YANAN;**
**DU, ZHIQIANG;**
**LI, QIN y**
**LI, MING**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

## DESCRIPCIÓN

Procedimiento y dispositivo de autenticación de entidad

**Campo**

La presente invención se refiere al campo de la seguridad de la red, y particularmente a un procedimiento y aparato para autenticar una entidad.

**Antecedentes**

La comunicación se realiza a través de una interfaz aérea en la tecnología de Comunicación de Campo Cercano (NFC) sin ningún contacto físico o tangible, y esta tecnología ha sufrido una variedad de amenazas de seguridad mientras se aplica ampliamente, por ejemplo, un atacante puede espiar e interceptar ilegalmente la información intercambiada entre dos partes de comunicación; duplicar o falsificar para hacerse pasar por una tarjeta legal; leer de forma remota información confidencial en una tarjeta utilizando un lector de tarjetas con alta potencia de radiofrecuencia, y luego descifrar utilizando un servidor de fondo con el fin de recuperar ilegalmente la información en la tarjeta, etc. En vista de estos ataques, la tecnología de NFC se proporcionará con una capacidad antifalsificación para aplicar un mecanismo de autenticación de las identidades de dos partes de la comunicación para autenticar así las identidades de la tarjeta y el lector a fin de garantizar la legalidad y autenticidad de las identidades de las dos partes de comunicación. Sin embargo, el mecanismo de autenticación de identidad ha estado ausente en la tecnología existente de comunicación de interfaz aérea NFC, resultando así en importantes riesgos de seguridad.

El documento US20130239174A1 divulga un módulo de seguridad que en un medio de grabación de datos, los datos que se escribirán en el medio de grabación de datos se cifran con una clave de contenido diferente de un dato a otro, y la clave de contenido se almacena de forma segura en el módulo de seguridad. Además, el módulo de seguridad realiza una autenticación mutua utilizando la tecnología de cifrado de clave pública con una unidad de disco para verificar que la contraparte sea una unidad autorizada (con licencia) y luego le da la clave de contenido a la contraparte, evitando así que los datos se filtren a cualquier unidad ilegal (sin licencia). De esta manera, es posible evitar que datos con derechos de autor como música de películas, etc. sean copiados ilegalmente (en contra del deseo del propietario de los datos).

El documento EP2234366A1 divulga un procedimiento de acceso de autenticación y un sistema de acceso de autenticación para una red inalámbrica de múltiples saltos. El equipo terminal y el coordinador tienen la capacidad de control de puertos, el coordinador difunde una trama de baliza, y el equipo terminal selecciona un conjunto de autenticación y gestión de claves y transmite un comando de solicitud de conexión al coordinador. El coordinador realiza la autenticación con el equipo terminal de acuerdo con el conjunto de autenticación y gestión de claves seleccionado por el equipo terminal, después de la autenticación, transmite un comando de respuesta de conexión al equipo terminal. El equipo terminal y el coordinador controlan el puerto de acuerdo con el resultado de autenticación, por lo tanto, se realiza el acceso autenticado para la red inalámbrica de múltiples saltos. La invención resuelve el problema de seguridad del procedimiento inalámbrico de autenticación de red de múltiples saltos.

**Sumario**

Las realizaciones de la invención proponen un procedimiento y aparato para autenticar una entidad para abordar el problema en la técnica anterior.

Un procedimiento para autenticar una entidad incluye:

la operación 1 de transmitir, por una entidad A, un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ a una entidad B, en el que $N_A$ representa un número aleatorio generado por la entidad A, y $Cert_A$ representa un certificado de la entidad A;

la operación 2 de verificar, por la entidad B, para la validez del certificado $Cert_A$ en el primer mensaje de autenticación de identidad de la entidad A al recibir el primer mensaje de autenticación de identidad, y si el certificado no es válido, luego terminando la autenticación;

la operación 3 de generar, por la entidad B, un número aleatorio $N_B$, y calculando una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_B$) utilizando su propia clave privada $CS_B$, en el que SIG representa un algoritmo de firma digital, $ID_A$ e $ID_B$ representan información de identificación de la entidad A y la entidad B respectivamente, $Q_B$ representa una clave pública temporal de la entidad B, y que transmite, por la entidad B, un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ para la entidad A, en el que $Cert_B$ representa un certificado de la entidad B;

la operación 4 de verificar, por la entidad A, para la exactitud de los datos de campo en el segundo mensaje de autenticación de identidad, incluidos $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad, y si los datos de campo son incorrectos como resultado de la verificación, luego terminando la autenticación;

la operación 5 de calcular, por la entidad A, una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_A$) de la entidad A utilizando su propia clave privada $CS_A$, en el que $Q_A$ representa una clave pública temporal de la entidad A; y verificar, por la entidad A, para ver si la clave pública temporal $Q_B$ de la entidad B ha sido almacenada, y si es así, luego usando el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, luego usando $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, luego terminando la autenticación;

la operación 6 de calcular, por la entidad A, información secreta z = f ($d_A$, $Q_B$) utilizando una clave privada temporal $d_A$ generada de antemano por la entidad A, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, en el que f representa una función de cálculo clave, y si la información secreta se calcula por error, luego terminando, por la entidad A, la autenticación; en caso contrario, convirtiendo la información secreta calculada z en una cadena de caracteres Z, y calculando una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), en el que KDF representa un algoritmo de derivación clave, calcular, por la entidad A, un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), en el que MAC1 representa una función de cálculo de código de autenticación de mensaje, y transmitir, por la entidad A, un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ a la entidad B;

la operación 7 de verificar, por la entidad B, para la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad incluyendo $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad, y si los datos de campo son incorrectos como resultado de la verificación, luego terminando la autenticación;

la operación 8 de verificar, por la entidad B, para ver si la clave pública temporal $Q_A$ de la entidad A ha sido almacenada, y si es así, luego usando el $Q_A$ almacenado; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, luego usando $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, luego terminando la autenticación;

la operación 9 de calcular, por la entidad B, información secreta z = f ($d_B$, $Q_A$) utilizando una clave privada temporal $d_B$ generada de antemano por la entidad B, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, luego terminando la autenticación; en caso contrario, convirtiendo la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y comparándolo con $MacTag_A$ en el tercer mensaje de autenticación de identidad recibido transmitido por la entidad A, y si no son consistentes, luego terminando la autenticación; en caso contrario, determinar que la entidad A es legal, calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$), y transmitiendo un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ a la entidad A; y

la operación 10 de calcular, por la entidad A, $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) al recibir el cuarto mensaje de autenticación de identidad de la entidad B, y compararlo con $MacTag_B$ en el cuarto mensaje de autenticación de identidad recibido, y si no son consistentes, luego determinar que la entidad B es ilegal; si son consistentes, luego determinar que la entidad B es legal.

Un procedimiento operativo de una entidad A mientras se realiza la autenticación de entidad con una entidad B incluye las operaciones de:

generar un número aleatorio $N_A$ y transmitir un primer mensaje de autenticación de identidad que incluya $N_A$ ||| $Cert_A$ a la entidad B, en el que $Cert_A$ representa un certificado de la entidad A;

verificar la exactitud de los datos de campo en un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad, y si los datos de campo son incorrecto como resultado de la verificación, luego terminando la autenticación;

calcular una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || [$ID_B$ || $N_A$ || $N_B$ || $Q_A$) usando su propia clave privada $CS_A$ y clave pública temporal $Q_A$, y verificando si una clave pública temporal $Q_B$ de la entidad B tiene sido almacenado, y si es así, luego usando el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, luego usando $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, luego terminando la autenticación;

calcular la información secreta z = f ($d_A$, $Q_B$) utilizando una clave privada temporal $d_A$ generada de antemano, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, luego terminando la autenticación; en caso contrario, convirtiendo la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), y calculando un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y transmitiendo un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ a la entidad B; y

calcular $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) al recibir un cuarto mensaje de autenticación de identidad de la entidad B, y compararlo con $MacTag_B$ en el cuarto mensaje de autenticación de identidad recibido, y si no son consistentes, luego determinar que la entidad B es ilegal; si son consistentes, luego determinar que la entidad B

es legal;

en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

Un procedimiento operativo de una entidad B mientras se realiza la autenticación de entidad con una entidad A incluye las operaciones de:

verificar la validez de un certificado $Cert_A$ en un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ de la entidad A al recibir el primer mensaje de autenticación de identidad, y si el certificado no es válido, luego terminando la autenticación; en caso contrario, generando un número aleatorio $N_B$, calcular una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_B$) utilizando su propia clave privada $CS_B$ y clave pública temporal $Q_B$, y transmitiendo un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ a la entidad A, en el que $Cert_B$ representa el certificado;

verificar la exactitud de los datos de campo en un tercer mensaje de autenticación de identidad que incluye $N_A$ || NB || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad, y si los datos de campo en el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación, luego terminando la autenticación;

verificar para ver si se ha almacenado una clave pública temporal $Q_A$ de la entidad A, y si es así, luego usando el $Q_A$ almacenado; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, luego usando $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, luego terminando la autenticación; y

calcular información secreta z = f ($d_B$, $Q_A$) utilizando una clave privada temporal $d_B$ generada de antemano, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, luego terminando la autenticación; en caso contrario, convirtiendo la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y comparándolo con $MacTag_A$ en el tercer mensaje de autenticación de identidad recibido transmitido por la entidad A, y si no son consistentes, luego terminando la autenticación; en caso contrario, determinar que la entidad A es legal, calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$), y transmitiendo un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ a la entidad A;

en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

Un aparato para autenticar una entidad con otro aparato incluye una unidad de memoria, una unidad de procesamiento y una unidad transceptora, en el que:

la unidad de memoria está configurada para almacenar un certificado $Cert_A$ y una clave privada $CS_A$ del aparato;

la unidad de procesamiento está configurada para generar un número aleatorio $N_A$, una clave privada temporal $d_A$, y una clave pública temporal $Q_A$;

la unidad transceptora está configurada para transmitir un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ al otro aparato, y para recibir un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ transmitido por el otro aparato;

la unidad de procesamiento está configurada para verificar el segundo mensaje de autenticación de identidad recibido que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ del otro aparato, y si el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación, finalizar la autenticación;

la unidad de procesamiento está configurada para calcular una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_A$) utilizando la clave privada $CS_A$ y la clave pública temporal $Q_A$;

la unidad de procesamiento está configurada para verificar si se ha almacenado una clave pública temporal $Q_B$ del otro aparato, y si es así, usar el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, finalizar la autenticación;

la unidad de procesamiento está configurada para calcular información secreta z = f ($d_A$, $Q_B$) usando $d_A$, y la clave pública temporal $Q_B$ del otro aparato basado en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula correctamente, para convertir la información secreta calculada z en una cadena de caracteres Z, para calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), y para calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$);

la unidad transceptora está configurada además para transmitir un tercer mensaje de autenticación de identidad que incluye $N_A$ || NB || $Q_A$ || $Sig_A$ || $MacTag_A$ al otro aparato, y para recibir un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ transmitido por el otro aparato; y

la unidad de procesamiento está configurada para calcular $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$), para comparar el $MacTag_B$ calculado con el $MacTag_B$ transmitido por el otro aparato, y si son consistentes, determinar que la identidad del otro aparato es legal; y

en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador del aparato, $ID_B$ representa el identificador del otro aparato, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

Un aparato para autenticar una entidad con otro aparato incluye una unidad de memoria, una unidad de procesamiento y una unidad transceptora, en el que:

la unidad de memoria está configurada para almacenar un certificado $Cert_B$ y una clave privada $CS_B$ del aparato;

la unidad de procesamiento está configurada para generar un número aleatorio $N_B$, una clave privada temporal $d_B$, y una clave pública temporal $Q_B$;

la unidad transceptora está configurada para recibir un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ del otro aparato;

la unidad de procesamiento está configurada para verificar la validez de un certificado $Cert_A$ en el primer mensaje de autenticación de identidad recibido del otro aparato, y si el certificado no es válido, finalizar la autenticación; y para calcular una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_B$) utilizando la clave privada $CS_B$ y la clave pública temporal $Q_B$;

la unidad transceptora está configurada además para transmitir un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ al otro aparato, y para recibir un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ transmitido por el otro aparato;

la unidad de procesamiento está configurada para verificar el tercer mensaje de autenticación de identidad recibido, incluyendo $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$, y si el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación, finalizar la autenticación;

la unidad de procesamiento está configurada además para verificar si se ha almacenado una clave pública temporal $Q_A$ del otro aparato, y si es así, usar la $Q_A$ almacenada; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, finalizar la autenticación; y

la unidad de procesamiento está configurada para calcular información secreta z = f ($d_B$, $Q_A$) usando la clave privada temporal $d_B$, y la clave pública temporal $Q_A$ del otro aparato basado en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula correctamente, para convertir la información secreta calculada z en una cadena de caracteres Z, para calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), para calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y para comparar el $MacTag_A$ calculado con el $MacTag_A$ transmitido por el otro aparato, y si son consistentes, determinar que la identidad del otro aparato es legal, y para calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$); y

la unidad transceptora está configurada además para transmitir un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ al otro aparato;

en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador del otro aparato, $ID_B$ representa el identificador del aparato, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

Un efecto ventajoso de la invención radica en que:

La invención puede proporcionar el mecanismo de autenticación de identidad para dispositivos de comunicación de interfaz aérea que incluye dispositivos NFC para garantizar la legalidad y autenticidad de las identidades de las dos partes de comunicación, y puede aplicarse ampliamente en diversos campos.

**Breve descripción de los dibujos**

Los dibujos descritos aquí están destinados a proporcionar una mayor comprensión de la invención, y estos dibujos constituyen una parte de la invención, pero no pretenden limitar la invención. En los dibujos:

La figura 1 ilustra un diagrama de flujo esquemático de un procedimiento para autenticar una entidad de acuerdo con una realización de la invención;

La figura 2 ilustra un diagrama estructural esquemático de un aparato correspondiente a una entidad A de acuerdo con una realización de la invención; y
La figura 3 ilustra un diagrama estructural esquemático de un aparato correspondiente a una entidad B de acuerdo con una realización de la invención.

**Descripción detallada de las realizaciones**

Las realizaciones de la invención proporcionan un procedimiento y un aparato para autenticar una entidad. La invención se refiere a una entidad A y una entidad B, y antes de la autenticación, las dos partes de comunicación, incluida la entidad A y la entidad B, tienen sus respectivos certificados $Cert_A$ y $Cert_B$, claves privadas $CS_A$ y $CS_B$, y una capacidad para autenticar los certificados de legalidad entre sí, y han obtenido información de identificación mutua. Con referencia a la figura 1, un procedimiento para autenticar una entidad de acuerdo con una realización de la invención incluye las siguientes operaciones:

En la operación 1, una entidad A transmite un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ a una entidad B, en el que $N_A$ representa un número aleatorio generado por la entidad A, y $Cert_A$ representa un certificado de la entidad A. "||" aquí representa la concatenación entre campos sin limitar un orden secuencial de los campos. Además en la invención, los campos concatenados por "||" puede considerarse como un "grupo de campos". Debe observarse que el "grupo de campos" en la invención está abierto en que uno o más campos distintos de los campos en el "grupo de campos" ejemplificados en las realizaciones de la invención también pueden incluirse en el "grupo de campos".
En la operación 2, la entidad B verifica la validez del certificado $Cert_A$ en el primer mensaje de autenticación de identidad de la entidad A al recibir el primer mensaje de autenticación de identidad, y si el certificado no es válido, entonces la entidad B puede terminar la autenticación.
En la operación 3, la entidad B genera un número aleatorio $N_B$ y calcula una firma digital $Sig_B = SIG (CS_B, ID_A || ID_B || N_A || N_B || Q_B)$ utilizando su propia clave privada $CS_B$, en el que SIG representa un algoritmo de firma digital, $ID_A$ e $ID_B$ representan información de identificación de la entidad A y la entidad B respectivamente, $Q_B$ representa una clave pública temporal de la entidad B, y la entidad B transmite un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ a la entidad A, en el que $Cert_B$ representa un certificado de la entidad B.
En la operación 4, la entidad A verifica la exactitud de los datos de campo en el segundo mensaje de autenticación de identidad, incluyendo $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad, y si los datos de campo son incorrectos como resultado de la verificación, entonces la entidad A puede terminar la autenticación.
En la operación 5, la entidad A calcula una firma digital $Sig_A = SIG (CS_A, ID_A || ID_B || N_A || N_B || Q_A)$ utilizando su propia clave privada $CS_A$, en el que $Q_A$ representa una clave pública temporal de la entidad A. La entidad A verifica si la clave pública temporal $Q_B$ de la entidad B ha sido almacenada y, de ser así, entonces la entidad A puede usar la $Q_B$ almacenada; en caso contrario, la entidad A puede verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, entonces la entidad A puede usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, entonces la entidad A puede terminar la autenticación.
En la operación 6, la entidad A calcula información secreta $z = f (d_A, Q_B)$ utilizando una clave privada temporal $d_A$ generada de antemano por la entidad A, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, en el que f representa una función de cálculo clave, y si la información secreta se calcula por error, entonces la entidad A puede terminar la autenticación; en caso contrario, la entidad A puede convertir la información secreta calculada z en una cadena de caracteres Z y calcular una clave $MK = KDF (N_A, N_B, Z, ID_A, ID_B)$, en el que KDF representa un algoritmo de derivación clave, la entidad A puede calcular un código de autenticación de mensaje $MacTag_A = MAC1 (MK, ID_A, ID_B, Q_A, Q_B)$, en el que MAC1 representa una función de cálculo de código de autenticación de mensaje, y la entidad A puede transmitir un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ a la entidad B.
En la operación 7, la entidad B verifica la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad incluyendo $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad, y si los datos de campo en el tercer mensaje de autenticación de identidad son incorrectos como resultado de la verificación, entonces la entidad B puede terminar la autenticación.
En la operación 8, la entidad B verifica si la clave pública temporal $Q_A$ de la entidad A ha sido almacenada y, de ser así, entonces la entidad B puede usar la $Q_A$ almacenada; en caso contrario, la entidad B puede verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, entonces la entidad B puede usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, entonces la entidad B puede terminar la autenticación.
En la operación 9, la entidad B calcula información secreta $z = f (d_B, Q_A)$ utilizando una clave privada temporal $d_B$ generada de antemano por la entidad B, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, entonces la entidad B puede terminar la autenticación; en caso contrario, la entidad B puede convertir la información secreta calculada z en una cadena de caracteres Z, calcular una clave $MK = KDF (N_A, N_B, Z, ID_A, ID_B)$, calcular un código de autenticación de mensaje $MacTag_A = MAC1 (MK, ID_A, ID_B, Q_A, Q_B)$, y compárelo con $MacTag_A$ en el tercer mensaje de autenticación de identidad recibido transmitido por la entidad A, y si no son consistentes, entonces la entidad B puede terminar la autenticación; en caso contrario, la entidad B puede determinar que la entidad A es legal, calcular un código de

autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) y transmite un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ a la entidad A.
En la operación 10, la entidad A calcula $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) al recibir el cuarto mensaje de autenticación de identidad de la entidad B, y lo compara con $MacTag_B$ en el cuarto mensaje de autenticación de identidad recibido, y si no son consistentes, entonces la entidad A puede determinar que la entidad B es ilegal; si son consistentes, entonces la entidad A puede determinar que la entidad B es legal.

Hasta aquí termina la autenticación.

Particularmente en la operación 4 anterior, la entidad A verifica la exactitud de los datos de campo en el segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad de la siguiente manera:

4.1. La entidad A verifica si el número aleatorio $N_A$ en el segundo mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_A$ transmitido por la entidad A a la entidad B, y si no son consistentes, entonces los datos del campo pueden ser incorrectos como resultado de la verificación;
4.2. La entidad A verifica la validez del $Cert_B$ en el segundo mensaje de autenticación de identidad, y si no es válido, entonces los datos del campo pueden ser incorrectos como resultado de la verificación; y
4.3. La entidad A verifica el $Sig_B$ usando una clave pública $CP_B$ de la entidad B para verificar la legalidad de la entidad B, y si la entidad B no es legal, entonces los datos del campo pueden ser incorrectos como resultado de la verificación, en el que la clave pública $CP_B$ de la entidad B está incluida en el certificado $Cert_B$ de la entidad B.

Cabe señalar que los controles anteriores no se limitarán a ningún pedido estrictamente requerido, y si alguno de los controles muestra incorrección, entonces se puede determinar que $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ recibido por la entidad A es incorrecto como resultado de la verificación.

Particularmente en la operación 7 anterior, la entidad B verifica la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad incluye:

7.1. La entidad B verifica si el número aleatorio $N_A$ en el tercer mensaje de autenticación de identidad recibido es consistente con el último número aleatorio recibido $N_A$, y si no son consistentes, entonces los datos del campo pueden ser incorrectos como resultado de la verificación;
7,2. La entidad B verifica si el número aleatorio $N_B$ en el tercer mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_B$ transmitido por la entidad B a la entidad A, y si no son consistentes, entonces los datos del campo pueden ser incorrectos como resultado de la verificación; y
7,3. La entidad B verifica el $Sig_A$ usando una clave pública $CP_A$ de la entidad A para verificar la legalidad de la entidad A, y si la entidad A no es legal, entonces los datos del campo pueden ser incorrectos como resultado de la verificación, en el que la clave pública $CP_A$ de la entidad A está incluida en el certificado $Cert_A$ de la entidad A.

Cabe señalar que los controles anteriores no se limitarán a ningún pedido estrictamente requerido, y si alguno de los controles muestra incorrección, entonces se puede determinar que $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ recibido por la entidad B es incorrecto como resultado de la verificación.

Además del procedimiento anterior para autenticar una entidad, una realización de la invención proporciona además un procedimiento operativo de la entidad A para realizar el procedimiento anterior, en el que el procedimiento operativo incluye las siguientes operaciones:

La entidad A genera un número aleatorio $N_A$ y transmite un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ a la entidad B, en el que $Cert_A$ representa un certificado de la entidad A;
La entidad A verifica la exactitud de los datos de campo en un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad, y si los datos de campo son incorrectos como resultado de la verificación, entonces la entidad A puede terminar la autenticación;
La entidad A calcula una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_A$) de la entidad A utilizando su propia clave privada $CS_A$ y clave pública temporal $Q_A$, y comprueba si una clave pública temporal $Q_B$ del la entidad B ha sido almacenada, y si es así, entonces la entidad A puede usar la $Q_B$ almacenada; en caso contrario, la entidad A puede verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, entonces la entidad A puede usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, entonces la entidad A puede terminar la autenticación;
La entidad A calcula información secreta z = f ($d_A$, $Q_B$) utilizando una clave privada temporal $d_A$ generada de antemano, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, entonces la entidad A puede terminar la autenticación; en caso contrario, la entidad A puede convertir la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$) y transmite un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ a la entidad B; y

La entidad A calcula $MacTag_s$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) al recibir un cuarto mensaje de autenticación de identidad de la entidad B, y lo compara con $MacTag_B$ en el cuarto mensaje de autenticación de identidad recibido, y si no son consistentes, entonces la entidad A puede determinar que la entidad B es ilegal; si son consistentes, entonces la entidad A puede determinar que la entidad B es legal.

Hasta aquí termina la autenticación.

Aquí SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

En particular, la entidad A verifica la exactitud de los datos de campo en el segundo mensaje de autenticación de identidad, incluidos $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad de la siguiente manera:

La entidad A verifica si el número aleatorio $N_A$ en el segundo mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_A$ transmitido por la entidad A a la entidad B, y si no son consistentes, entonces los datos del campo pueden ser incorrectos como resultado de la verificación;
La entidad A verifica la validez del $Cert_B$ en el segundo mensaje de autenticación de identidad, y si no es válido, entonces los datos del campo pueden ser incorrectos como resultado de la verificación; y
La entidad A verifica el $Sig_B$ usando una clave pública $CP_B$ de la entidad B para verificar la legalidad de la entidad B, y si la entidad B no es legal, entonces los datos del campo pueden ser incorrectos como resultado de la verificación, en el que la clave pública $CP_B$ de la entidad B se incluye en un certificado $Cert_B$ de la entidad B.

Cabe señalar que los controles anteriores no se limitarán a ningún pedido estrictamente requerido, y si alguno de los controles muestra incorrección, entonces se puede determinar que el $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ recibido es incorrecto como resultado de la verificación.

Además del procedimiento anterior para autenticar una entidad, una realización de la invención proporciona además un procedimiento operativo para la entidad B al realizar el procedimiento, en el que el procedimiento operativo incluye las siguientes operaciones:

La entidad B verifica la validez de un certificado $Cert_A$ en un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ de la entidad A al recibir el primer mensaje de autenticación de identidad, y si el certificado no es válido, entonces la entidad B puede terminar la autenticación; en caso contrario, la entidad B puede generar un número aleatorio $N_B$, calcular una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_B$) utilizando su propia clave privada $CS_B$ y clave pública temporal $Q_B$, y transmite un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ a la entidad A, en el que $Cert_B$ representa el certificado;
La entidad B verifica la exactitud de los datos de campo en un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad, y si los datos de campo en el tercer mensaje de autenticación de identidad son incorrectos como resultado de la verificación, entonces la entidad B puede terminar la autenticación;
La entidad B verifica si se ha almacenado una clave pública temporal $Q_A$ de la entidad A y, de ser así, entonces la entidad B puede usar la $Q_A$ almacenada; en caso contrario, la entidad B puede verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, entonces la entidad B puede usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, entonces la entidad B puede terminar la autenticación; y
La entidad B calcula información secreta z = f ($d_B$, $Q_A$) utilizando una clave privada temporal $d_B$ generada de antemano, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, entonces la entidad B puede terminar la autenticación; en caso contrario, la entidad B puede convertir la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y compárelo con $MacTag_A$ en el tercer mensaje de autenticación de identidad recibido transmitido por la entidad A, y si no son consistentes, entonces la entidad B puede terminar la autenticación; en caso contrario, la entidad B puede determinar que la entidad A es legal, calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) y transmite un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ a la entidad A.

Aquí SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

En particular, la entidad B verifica la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad, incluyendo $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad incluye:

La entidad B verifica si el número aleatorio $N_A$ en el tercer mensaje de autenticación de identidad recibido es consistente con el último número aleatorio recibido $N_A$, y si no son consistentes, entonces los datos del campo

pueden ser incorrectos como resultado de la verificación;
La entidad B verifica si el número aleatorio $N_B$ en el tercer mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_B$ transmitido por la entidad B a la entidad A, y si no son consistentes, entonces los datos del campo pueden ser incorrectos como resultado de la verificación; y
La entidad B verifica el $Sig_A$ usando una clave pública $CP_A$ de la entidad A para verificar la legalidad de la entidad A, y si la entidad A no es legal, entonces los datos del campo pueden ser incorrectos como resultado de la verificación, en el que la clave pública $CP_A$ de la entidad A está incluida en el certificado $Cert_A$ de la entidad A.

Cabe señalar que los controles anteriores no se limitarán a ningún pedido estrictamente requerido, y si alguno de los controles muestra incorrección, entonces se puede determinar que el $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ recibido es incorrecto como resultado de la verificación.

Con referencia a la figura 2, además del procedimiento anterior para autenticar una entidad, una realización de la invención proporciona además un aparato, correspondiente a la entidad A, para realizar el procedimiento anterior, en el que el aparato incluye una unidad 201 de memoria, una unidad 202 de procesamiento y una unidad 203 transceptora, en el que:

La unidad 201 de memoria está configurada para almacenar un certificado $Cert_A$ y una clave privada $CS_A$;
La unidad 202 de procesamiento está configurada para generar un número aleatorio $N_A$, una clave privada temporal $d_A$, y una clave pública temporal $Q_A$;
La unidad 203 transceptora está configurada para transmitir un primer mensaje de autenticación de identidad que incluye $N_A$ || $Cert_A$ a la entidad B, y para recibir un segundo mensaje de autenticación de identidad que incluye $N_A$ | $N_B$ | $Cert_B$ | $Q_B$ | $Sig_B$ transmitido por la entidad B; La unidad 202 de procesamiento está configurada además para verificar el segundo mensaje de autenticación de identidad recibido que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B, y si el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación, finalizar la autenticación;
La unidad 202 de procesamiento está configurada además para calcular una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_A$) utilizando la clave privada $CS_A$ y la clave pública temporal $Q_A$;
La unidad 202 de procesamiento está configurada además para verificar si se ha almacenado una clave pública temporal $Q_B$ del otro aparato, y si es así, usar el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, finalizar la autenticación;
La unidad 202 de procesamiento está configurada además para calcular información secreta z = f ($d_A$, $Q_B$ ) utilizando $d_A$, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula correctamente, para convertir la información secreta calculada z en una cadena de caracteres Z, para calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), y para calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$);
La unidad 203 transceptora está configurada además para transmitir un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ a la entidad B, y para recibir un cuarto mensaje de autenticación de identidad que incluye MacTagB transmitido por la entidad B; y la unidad 202 de procesamiento está configurada además para calcular $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$), para comparar el $MacTag_B$ calculado con el $MacTag_B$ transmitido por la entidad B, y si son consistentes, determinar que la identidad de la entidad B es legal; y
Aquí SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador del aparato, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

En particular, la unidad 202 de procesamiento configurada para verificar el segundo mensaje de autenticación de identidad recibido que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B está configurada:

Para verificar si el número aleatorio $N_A$ en el segundo mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_A$ transmitido por la entidad A a la entidad B, y si no son consistentes, determinar que el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación; Para verificar la validez del $Cert_B$ en el segundo mensaje de autenticación de identidad, y si no es válido, determinar que el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación; y
Para verificar $Sig_B$ utilizando una clave pública $CP_B$ de la entidad B verificar la legalidad de la entidad B, y si la entidad B no es legal, determinar que el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación, en el que la clave pública $CP_B$ de la entidad B se incluye en un certificado $Cert_B$ de la entidad B.

Cabe señalar que los controles anteriores no se limitarán a ningún pedido estrictamente requerido, y si alguno de los controles muestra incorrección, entonces se puede determinar que el $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ recibido es incorrecto como resultado de la verificación.

Con referencia a la figura 3, además del procedimiento anterior para autenticar una entidad, una realización de la invención proporciona además un aparato, correspondiente a la entidad B, para realizar el procedimiento anterior, en el que el aparato incluye una unidad 301 de memoria, una unidad 302 de procesamiento y una unidad 303

transceptora, en el que:

La unidad 301 de memoria está configurada para almacenar un certificado $Cert_B$ y una clave privada $CS_B$;
La unidad 302 de procesamiento está configurada para generar un número aleatorio $N_B$, una clave privada temporal $d_B$, y una clave pública temporal $Q_B$;
La unidad 303 transceptora está configurada para recibir un primer mensaje de autenticación de identidad que incluye $N_A$ || [$Cert_A$ de la entidad A;
La unidad 302 de procesamiento está configurada para verificar la validez de un certificado $Cert_A$ en el primer mensaje de autenticación de identidad recibido de la entidad A, y si el certificado no es válido, finalizar la autenticación; y para calcular una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_B$) utilizando la clave privada $CS_B$ y la clave pública temporal $Q_B$;
La unidad 303 transceptora está configurada además para transmitir un segundo mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ a la entidad A, y para recibir un tercer mensaje de autenticación de identidad que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || MacTag $_A$ transmitida por la entidad A;
La unidad 302 de procesamiento está configurada además para verificar el tercer mensaje de autenticación de identidad recibido que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$, y si el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación, finalizar la autenticación; La unidad 302 de procesamiento está configurada además para verificar si se ha almacenado una clave pública temporal $Q_A$ del otro aparato, y si es así, usar la $Q_A$ almacenada; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, finalizar la autenticación; y
La unidad 302 de procesamiento está configurada además para calcular información secreta z = f ($d_B$, $Q_A$) utilizando la clave privada temporal $d_B$, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula correctamente, para convertir la información secreta calculada z en una cadena de caracteres Z, para calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), para calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y para comparar el $MacTag_A$ calculado con el $MacTag_A$ transmitido por la entidad A, y si son consistentes, determinar que la identidad de la entidad A es legal, y para calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$); y
La unidad 303 transceptora está configurada además para transmitir un cuarto mensaje de autenticación de identidad que incluye $MacTag_B$ a la entidad A.

Aquí SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

En particular, la unidad 302 de procesamiento configurada para verificar el tercer mensaje de autenticación de identidad recibido que incluye $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad está configurado:

Para verificar si el número aleatorio $N_A$ en el tercer mensaje de autenticación de identidad recibido es consistente con el último número aleatorio recibido $N_A$, y si no son consistentes, determinar que el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación;
Para verificar si el número aleatorio $N_B$ en el tercer mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_B$ transmitido por la entidad B a la entidad A, y si no son consistentes, determinar que el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación; y
Para verificar $Sig_A$ utilizando una clave pública $CP_A$ de la entidad A verificar la legalidad de la entidad A, y si la entidad A no es legal, determinar que el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación, en el que la clave pública $CP_A$ de la entidad A está incluida en el certificado $Cert_A$ de la entidad A.

Cabe señalar que los controles anteriores no se limitarán a ningún pedido estrictamente requerido, y si alguno de los controles muestra incorrección, entonces se puede determinar que el $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ recibido es incorrecto como resultado de la verificación.

En resumen, las realizaciones de la invención permiten la autenticación de identidad entre entidades con una función de negociación sobre una clave, y pueden aplicarse ampliamente en diversos campos. Las realizaciones de la invención pueden ser aplicables a la identificación por radiofrecuencia (RFID), una red de sensores inalámbricos (WSN), comunicación de campo cercano (NFC), una tarjeta sin contacto, una red de área local inalámbrica (WLAN) y otros campos de comunicación a través de una interfaz aérea. La entidad A y la entidad B pueden ser un lector de tarjetas y una etiqueta en el campo de RFID, nodos en las redes inalámbricas de sensores, dispositivos terminales en el campo de NFC, un lector de tarjetas y una tarjeta en el campo de las tarjetas sin contacto, un terminal y un punto de acceso en la red de área local inalámbrica, etc.

Además, en una realización preferida de la invención, si la solución técnica de acuerdo con la invención se aplica al campo de NFC, entonces la entidad A puede transmitir el primer mensaje de autenticación de identidad a la entidad B después de encapsularlo en una unidad de datos de protocolo ACT_REQ, la entidad B puede transmitir el segundo

mensaje de autenticación de identidad a la entidad A después de encapsularlo en una unidad de datos de protocolo ACT_RES, la entidad A puede transmitir el tercer mensaje de autenticación de identidad a la entidad B después de encapsularlo en una unidad de datos de protocolo VFY_REQ, y la entidad B puede transmitir el cuarto mensaje de autenticación de identidad a la entidad A después de encapsularlo en una unidad de datos de protocolo VFY_RES, en el que ACT_REQ, ACT_RES, VFY_REQ y VFY_RES son formatos de unidades de datos de protocolo definidos de acuerdo con la norma ISO/IEC 13157-1. Después de que los mensajes de autenticación de identidad se encapsulan como tales, habrá una mejor compatibilidad de la solución técnica de acuerdo con la invención con otros mecanismos de seguridad NFC existentes.

Los expertos en la materia apreciarán que las formas de realización de la invención pueden realizarse como un procedimiento, un sistema o un producto de programa informático. Por lo tanto, la invención se puede realizar en forma de una forma de realización completamente de hardware, en una forma de realización completamente de software o en una forma de realización de software y hardware en combinación. Adicionalmente, la invención se puede realizar en forma de un producto de programa informático realizado en uno o más medios de almacenamiento utilizables por ordenador (incluyendo, pero no limitándose a memoria de disco, un CD-ROM, una memoria óptica, etc.) en la que se contienen los códigos de programas utilizables por ordenador.

La invención se ha descrito en un diagrama de flujo y/o un diagrama de bloques del procedimiento, el dispositivo (sistema) y el producto de programa informático de acuerdo con las realizaciones de la invención. Cabe apreciar que los respectivos flujos y/o bloques en el diagrama de flujo y/o diagrama de bloques y combinaciones de los flujos y/o bloques en el diagrama de flujo y/o el diagrama de bloques pueden realizarse en instrucciones de programa informático. Estas instrucciones de programa informático pueden cargarse en un ordenador de uso general, un ordenador de uso específico, un procesador integrado o un procesador de otro dispositivo de tratamiento de datos programable para producir una máquina de modo que las instrucciones ejecutadas en el ordenador o el procesador de otro dispositivo de tratamiento de datos programable crean medios para realizar funciones específicas en el(los) flujo(s) del diagrama de flujo y/o el(los) bloque(s) del diagrama de bloques.

Estas instrucciones de programa informático también se pueden almacenar en una memoria legible por ordenador capaz de dirigir el ordenador o el dispositivo de tratamiento de datos programables para operar de una manera específica, de manera que las instrucciones almacenadas en la memoria legible por ordenador crean un artículo de fabricación que incluye medios de instrucción que realizan funciones especificadas en el(los) flujo(s) y/o bloque(s) del diagrama de bloques.

Estas instrucciones de programa informático también se pueden cargar en un ordenador y otro dispositivo de tratamiento de datos programable para que una serie de operaciones operacionales se realicen en el ordenador o el otro dispositivo de tratamiento de datos programable para crear un procedimiento implementado por ordenador para que las instrucciones ejecutadas en el ordenador o el otro dispositivo programable proporcionen operaciones para realizar las funciones especificadas en el(los) flujo(s) del diagrama de flujo y/o el(los) bloque(s) del diagrama de bloques.

Aunque las formas de realización preferentes de la invención se han descrito, los expertos en la materia que se benefician del concepto subyacente inventivo pueden realizar las modificaciones y las variaciones adicionales a esas formas de realización. Por lo tanto, las reivindicaciones adjuntas pretenden construirse como que abarcan las formas de realización preferentes y todas las modificaciones y variaciones que entran dentro del ámbito de la invención.

Evidentemente, los expertos en la materia pueden realizar diversas modificaciones y variaciones a la invención sin alejarse del ámbito de la invención. Por lo tanto, la invención también pretende abarcar estas modificaciones y variaciones siempre que las modificaciones y las variaciones entren dentro del ámbito de las reivindicaciones adjuntas a la invención y sus equivalentes.

**REIVINDICACIONES**

1. Un procedimiento para autenticar una entidad, comprendiendo el procedimiento:

la operación 1 de transmitir, por una entidad A, un primer mensaje de autenticación de identidad que comprende $N_A$ || $Cert_A$ a una entidad B, en el que $N_A$ representa un número aleatorio generado por la entidad A, y $Cert_A$ representa un certificado de la entidad A;
la operación 2 de verificar, por la entidad B, la validez del certificado $Cert_A$ en el primer mensaje de autenticación de identidad de la entidad A tras recibir el primer mensaje de autenticación de identidad, y si el certificado no es válido, después terminar la autenticación;
la operación 3 de generar, por la entidad B, un número aleatorio $N_B$, y calcular una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_B$) utilizando su propia clave privada $CS_B$, en el que SIG representa un algoritmo de firma digital, $ID_A$ e $ID_B$ representan información de identificación de la entidad A y la entidad B respectivamente, $Q_B$ representa una clave pública temporal de la entidad B, y que transmite, por la entidad B, un segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ para la entidad A, en el que $Cert_B$ representa un certificado de la entidad B; la operación 4 de verificar, por la entidad A, la exactitud de los datos de campo en el segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad, y si los datos de campo son incorrectos como resultado de la verificación, después terminar la autenticación;
la operación 5 de calcular, por la entidad A, una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_A$) de la entidad A utilizando su propia clave privada $CS_A$, en el que $Q_A$ representa una clave pública temporal de la entidad A; y verificar, por la entidad A, para ver si la clave pública temporal $Q_B$ de la entidad B ha sido almacenada, y si es así, después usar el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, después usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, después terminar la autenticación;
la operación 6 de calcular, por la entidad A, información secreta z = f ($d_A$, $Q_B$) utilizando una clave privada temporal $d_A$ generada de antemano por la entidad A, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, en el que f representa una función de cálculo clave, y si la información secreta se calcula por error, después terminar, por la entidad A, la autenticación; en caso contrario, convirtir la información secreta calculada z en una cadena de caracteres Z, y calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), en el que KDF representa un algoritmo de derivación clave, calcular, por la entidad A, un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), en el que MAC1 representa una función de cálculo de código de autenticación de mensaje, y transmitir, por la entidad A, un tercer mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ para la entidad B;
la operación 7 de verificar, por la entidad B, la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad, y si los datos de campo son incorrectos como resultado de la verificación, después terminar la autenticación;
la operación 8 de verificar, por la entidad B, para ver si la clave pública temporal $Q_A$ de la entidad A ha sido almacenada, y si es así, después usar el $Q_A$ almacenado; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, después usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, después terminar la autenticación;
la operación 9 de calcular, por la entidad B, información secreta z = f ($d_B$, $Q_A$) utilizando una clave privada temporal $d_B$ generada de antemano por la entidad B, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, después terminar la autenticación; en caso contrario, convertir la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y comparándolo con $MacTag_A$ en el tercer mensaje de autenticación de identidad recibido transmitido por la entidad A, y si no son consistentes, después terminar la autenticación; en caso contrario, determinar que la entidad A es legal, calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$), y transmitir un cuarto mensaje de autenticación de identidad que comprende $MacTag_B$ a la entidad A; y
la operación 10 de calcular, por la entidad A, $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) tras recibir el cuarto mensaje de autenticación de identidad de la entidad B, y compararlo con $MacTag_B$ en el cuarto mensaje de autenticación de identidad recibido, y si no son consistentes, después determinar que la entidad B es ilegal; si son consistentes, después determinar que la entidad B es legal.

2. El procedimiento de acuerdo con la reivindicación 1, en el que en la operación 4, verificar, por la entidad A, la corrección de los datos de campo en el segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B al recibir el segundo mensaje de autenticación de identidad comprende:

4.1. verificar, por la entidad A, si el número aleatorio $N_A$ en el segundo mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_A$ transmitido por la entidad A a la entidad B, y si no son consistentes, después determinar que los datos del campo no son incorrectos como resultado de la verificación;
4.2. verificar, por la entidad A, $Cert_B$ en el segundo mensaje de autenticación de identidad para validez, y si no es válido, después determinar que los datos del campo no son incorrectos como resultado de la verificación; y
4.3. verificar, por la entidad A, $Sig_B$ usando una clave pública $CP_B$ de la entidad B para verificar la legalidad de la entidad B, y si la entidad B no es legal, después determinar que los datos del campo no son incorrectos como

resultado de la verificación, en el que la clave pública $CP_B$ de la entidad B está comprendida en el certificado $Cert_B$ de la entidad B;

en el que si uno cualquiera de los controles muestra incorrección, entonces se determina que $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ recibido por la entidad A es incorrecto como resultado de la verificación.

3. El procedimiento de acuerdo con la reivindicación 1, en el que en la operación 7, verificar, por la entidad B, para la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A tras recibir el tercer mensaje de autenticación de identidad comprende:

7.1. verificar, por la entidad B, si el número aleatorio $N_A$ en el tercer mensaje de autenticación de identidad recibido es consistente con el último número aleatorio recibido $N_A$, y si no son consistentes, después determinar que los datos del campo no son incorrectos como resultado de la verificación;
7.2. verificar, por la entidad B, si el número aleatorio $N_B$ en el tercer mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_B$ transmitido por la entidad B a la entidad A, y si no son consistentes, después determinar que los datos del campo no son incorrectos como resultado de la verificación; y
7.3. verificar, por la entidad B, $Sig_A$ usando una clave pública $CP_A$ de la entidad A para verificar la legalidad de la entidad A, y si la entidad A no es legal, después determinar que los datos del campo no son incorrectos como resultado de la verificación, en el que la clave pública $CP_A$ de la entidad A está comprendida en el certificado $Cert_A$ de la entidad A;

en el que si uno cualquiera de los controles muestra incorrección, entonces se determina que $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ recibido por la entidad B es incorrecto como resultado de la verificación.

4. Un procedimiento operativo de una entidad A mientras se realiza la autenticación de entidad con una entidad B, comprendiendo el procedimiento las operaciones de:

generar un número aleatorio $N_A$ y transmitir un primer mensaje de autenticación de identidad que comprende $N_A$ || $Cert_A$ a la entidad B, en el que $Cert_A$ representa un certificado de la entidad A;
verificar la exactitud de los datos de campo en un segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B tras recibir el segundo mensaje de autenticación de identidad, y si los datos de campo son incorrecto como resultado de la verificación, después terminar la autenticación;
calcular una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || $ID_B$ || $N_A$ || $N_B$ || $Q_A$) utilizando su propia clave privada $CS_A$ y clave pública temporal $Q_A$, y verificar si se ha utilizado una clave pública temporal $Q_B$ de la entidad B almacenado, y si es así, después usar el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, después usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, después terminar la autenticación;
calcular la información secreta z = f ($d_A$, $Q_B$) utilizando una clave privada temporal $d_A$ generada de antemano, y la clave pública temporal $Q_B$ de la entidad B basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, después terminar la autenticación; en caso contrario, convertir la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), y calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y transmitiendo un tercer mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ a la entidad B; y
calcular $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$) tras recibir un cuarto mensaje de autenticación de identidad de la entidad B, y compararlo con $MacTag_B$ en el cuarto mensaje de autenticación de identidad recibido, y si no son consistentes, después determinar que la entidad B es ilegal; si son consistentes, después determinar que la entidad B es legal;
en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

5. El procedimiento de acuerdo con la reivindicación 4, en el que la verificación de la exactitud de los datos de campo en el segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ de la entidad B tras recibir el segundo mensaje de autenticación de identidad comprende:

verificar si el número aleatorio $N_A$ en el segundo mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_A$ transmitido por la entidad A a la entidad B, y si no son consistentes, después determinar que los datos del campo son incorrectos como resultado de la verificación; verificar la validez del $Cert_B$ en el segundo mensaje de autenticación de identidad y, si no es válido, después determinar que los datos del campo son incorrectos como resultado de la verificación; y
verificar $Sig_B$ utilizando una clave pública $CP_B$ de la entidad B para verificar la legalidad de la entidad B, y si la entidad B no es legal, determinar que los datos del campo son incorrectos como resultado de la verificación, en el que la clave pública $CP_B$ de la entidad B está comprendida en un certificado $Cert_B$ de la entidad B;
en el que si uno cualquiera de los controles muestra incorrección, entonces se determina que el $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ recibido es incorrecto como resultado de la verificación.

6. Un procedimiento operativo de una entidad B mientras se realiza la autenticación de entidad con una entidad A,

comprendiendo el procedimiento las operaciones de:

verificar la validez de un certificado $Cert_A$ en un primer mensaje de autenticación de identidad que comprende $N_A$ || $Cert_A$ de la entidad A al recibir el primer mensaje de autenticación de identidad, y si el certificado no es válido, después terminar la autenticación; en caso contrario, generar un número aleatorio $N_B$, calcular una firma digital $Sig_B$ = SIG ($CS_B$, $ID_A$ $IIID_B$ $IIN_A$ $IIN_B$ $IIQ_B$ ) utilizando su propia clave privada $CS_B$ y clave pública temporal $Q_B$, y transmitiendo un segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ a la entidad A, en el que $Cert_B$ representa el certificado;
verificar la exactitud de los datos de campo en un tercer mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad, y si los datos de campo en el tercer mensaje de autenticación de identidad son incorrectos como resultado de la verificación, después terminar la autenticación;
verificar para ver si se ha almacenado una clave pública temporal $Q_A$ de la entidad A, y si es así, después usar el $Q_A$ almacenado; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, después usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, después terminar la autenticación; y
calcular información secreta z = f ($d_B$, $Q_A$) utilizando una clave privada temporal $d_B$ generada de antemano, y la clave pública temporal $Q_A$ de la entidad A basada en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula por error, después terminar la autenticación; en caso contrario, convertir la información secreta calculada z en una cadena de caracteres Z, calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), calcular un código de autenticación de mensaje $MacTag_A$ = MAC1 (MK, $ID_A$, $ID_B$, $Q_A$, $Q_B$), y comparándolo con $MacTag_A$ en el tercer mensaje de autenticación de identidad recibido transmitido por la entidad A, y si no son consistentes, después terminar la autenticación; en caso contrario, determinar que la entidad A es legal, calcular un código de autenticación de mensaje $MacTag_B$ = MAC1 (MK, $ID_B$, $ID_A$, $Q_B$, $Q_A$), y transmitir un cuarto mensaje de autenticación de identidad que comprende $MacTag_B$ a la entidad A;
en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador de la entidad A, $ID_B$ representa el identificador de la entidad B, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

7. El procedimiento de acuerdo con la reivindicación 6, en el que la verificación de la exactitud de los datos de campo en el tercer mensaje de autenticación de identidad que comprende $N_A$ || NB || $Q_A$ || $Sig_A$ || $MacTag_A$ de la entidad A al recibir el tercer mensaje de autenticación de identidad comprende:

verificar si el número aleatorio $N_A$ en el tercer mensaje de autenticación de identidad recibido es coherente con el último número aleatorio recibido $N_A$, y si no son coherentes, después determinar que los datos del campo son incorrectos como resultado de la verificación;
verificar si el número aleatorio $N_B$ en el tercer mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_B$ transmitido por la entidad B a la entidad A, y si no son consistentes, después determinar que los datos del campo son incorrectos como resultado de la verificación; y verificar $Sig_A$ usando una clave pública $CP_A$ de la entidad A para verificar la legalidad de la entidad A, y si la entidad A no es legal, después determinar que los datos del campo son incorrectos como resultado de la verificación, en el que la clave pública $CP_A$ de la entidad A está comprendida en el certificado $Cert_A$ de la entidad A; en el que si uno cualquiera de los controles muestra incorrección, entonces se determina que el $N_A$ || NB || $Q_A$ || $Sig_A$ || $MacTag_A$ recibido es incorrecto como resultado de la verificación.

8. Un aparato para realizar la autenticación de entidad con otro aparato, comprendiendo el aparato una unidad de memoria, una unidad de procesamiento y una unidad transceptora, en el que:

la unidad de memoria está configurada para almacenar un certificado $Cert_A$ y una clave privada $CS_A$ del aparato;
la unidad de procesamiento está configurada para generar un número aleatorio $N_A$, una clave privada temporal $d_A$, y una clave pública temporal $Q_A$;
la unidad transceptora está configurada para transmitir un primer mensaje de autenticación de identidad que comprende $N_A$ || $Cert_A$ al otro aparato, y para recibir un segundo mensaje de autenticación de identidad que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ transmitido por el otro aparato;
la unidad de procesamiento está configurada además para verificar el segundo mensaje de autenticación de identidad recibido que comprende $N_A$ || $N_B$ || $Cert_B$ || $Q_B$ || $Sig_B$ del otro aparato, y si el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación, finalizar la autenticación;
la unidad de procesamiento está configurada además para calcular una firma digital $Sig_A$ = SIG ($CS_A$, $ID_A$ || [$ID_B$ || $N_A$ || $N_B$ || $Q_A$) utilizando la clave privada $CS_A$ y la clave pública temporal $Q_A$;
la unidad de procesamiento está configurada además para verificar si se ha almacenado una clave pública temporal $Q_B$ del otro aparato, y si es así, usar el $Q_B$ almacenado; en caso contrario, verificar la validez de $Q_B$ en el segundo mensaje de autenticación de identidad recibido, y si $Q_B$ es válido, usar $Q_B$ en el segundo mensaje de autenticación de identidad recibido; si $Q_B$ no es válido, finalizar la autenticación;
la unidad de procesamiento está configurada para calcular información secreta z = f ($d_A$, $Q_B$) usando $d_A$, y la clave pública temporal $Q_B$ del otro aparato basado en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula correctamente, convertir la información secreta calculada z en una cadena de caracteres Z, para calcular una clave MK = KDF ($N_A$, $N_B$, Z, $ID_A$, $ID_B$), y para calcular un código de autenticación de mensaje

$MacTagA = MAC1 (MK, ID_A, ID_B, Q_A, Q_B)$;
la unidad transceptora está configurada además para transmitir un tercer mensaje de autenticación de identidad que comprende $N_A \| N_B \| Q_A \| Sig_A \| MacTag_A$ al otro aparato, y para recibir un cuarto mensaje de autenticación de identidad que comprende $MacTag_B$ transmitido por el otro aparato; y
la unidad de procesamiento está configurada además para calcular $MacTag_B = MAC1 (MK, ID_B, ID_A, Q_B, Q_A)$, para comparar el $MacTag_B$ calculado con el $MacTag_B$ transmitido por el otro aparato, y si son consistentes, determinar que la identidad del otro aparato es legal; y
en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador del aparato, $ID_B$ representa el identificador del otro aparato, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

9. El aparato de acuerdo con la reivindicación 8, en el que la unidad de procesamiento configurada para verificar el segundo mensaje de autenticación de identidad recibido que comprende $N_A \| N_B \| Cert_B \| Q_B \| Sig_B$ del otro aparato está configurado para:

verificar si el número aleatorio $N_A$ en el segundo mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_A$ transmitido por el aparato al otro aparato, y si no son consistentes, determinar que el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación;
verificar la validez del $Cert_B$ en el segundo mensaje de autenticación de identidad, y si no es válido, determinar que el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación; y
verificar $Sig_B$ utilizando una clave pública $CP_B$ del otro aparato para verificar la legalidad del otro aparato, y si el otro aparato no es legal, determinar que el segundo mensaje de autenticación de identidad es incorrecto como resultado de la verificación, en el que la clave pública $CP_B$ del otro aparato está comprendida en un certificado $Cert_B$ del otro aparato;
en el que si uno cualquiera de los controles muestra incorrección, entonces se determina que el $N_A \| N_B \| Cert_B \| Q_B \| Sig_B$ recibido es incorrecto como resultado de la verificación.

10. Un aparato para realizar la autenticación de entidad con otro aparato, comprendiendo el aparato una unidad de memoria, una unidad de procesamiento y una unidad transceptora, en el que:

la unidad de memoria está configurada para almacenar un certificado $Cert_B$ y una clave privada $CS_B$ del aparato;
la unidad de procesamiento está configurada para generar un número aleatorio $N_B$, una clave privada temporal $d_B$, y una clave pública temporal $Q_B$;
la unidad transceptora está configurada para recibir un primer mensaje de autenticación de identidad que comprende $N_A \| Cert_A$ del otro aparato;
la unidad de procesamiento está configurada para verificar la validez de un certificado $Cert_A$ en el primer mensaje de autenticación de identidad recibido del otro aparato, y si el certificado no es válido, finalizar la autenticación; y calcular una firma digital $Sig_B = SIG (CS_B, ID_A \| ID_B \| N_A \| N_B \| Q_B)$ utilizando la clave privada $CS_B$ y la clave pública temporal $Q_B$;
la unidad transceptora está configurada además para transmitir un segundo mensaje de autenticación de identidad que comprende $N_A \| N_B \| Cert_B \| Q_B \| Sig_B$ al otro aparato, y para recibir un tercer mensaje de autenticación de identidad que comprende $N_A \| N_B \| Q_A \| Sig_A \| MacTag_A$ transmitido por el otro aparato; la unidad de procesamiento está configurada para verificar el tercer mensaje de autenticación de identidad recibido que comprende $N_A \| N_B \| Q_A \| Sig_A \| MacTag_A$, y si el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación, finalizar la autenticación;
la unidad de procesamiento está configurada además para verificar si se ha almacenado una clave pública temporal $Q_A$ del otro aparato, y si es así, usar la $Q_A$ almacenada; en caso contrario, verificar la validez de $Q_A$ en el tercer mensaje de autenticación de identidad recibido, y si $Q_A$ es válido, usar $Q_A$ en el tercer mensaje de autenticación de identidad recibido; si $Q_A$ no es válido, finalizar la autenticación; y
la unidad de procesamiento está configurada además para calcular información secreta $z = f (d_B, Q_A)$ usando la clave privada temporal $d_B$, y la clave pública temporal $Q_A$ del otro aparato basado en el protocolo de intercambio de claves ECDH, y si la información secreta se calcula correctamente, para convertir la información secreta calculada z en una cadena de caracteres Z, para calcular una clave $MK = KDF (N_A, N_B, Z, ID_A, ID_B)$, para calcular un código de autenticación de mensaje $MacTag_A = MAC1 (MK, ID_A, ID_B, Q_A, Q_B)$, y para comparar el $MacTag_A$ calculado con el $MacTag_A$ transmitido por el otro aparato, y si son consistentes, determinar que la identidad del otro aparato es legal, y para calcular un código de autenticación de mensaje $MacTag_B = MAC1 (MK, ID_B, ID_A, Q_B, Q_A)$; y
la unidad transceptora está configurada además para transmitir un cuarto mensaje de autenticación de identidad que comprende $MacTag_B$ al otro aparato; en el que SIG representa un algoritmo de firma digital, $ID_A$ representa el identificador del otro aparato, $ID_B$ representa el identificador del aparato, f representa una función de cálculo clave, KDF representa una función de derivación de clave, y MAC1 es una función de cálculo de código de autenticación de mensaje.

11. El aparato de acuerdo con la reivindicación 10, en el que la unidad de procesamiento configurada para verificar el tercer mensaje de autenticación de identidad recibido que comprende $N_A \| N_B \| Q_A \| Sig_A \| MacTag_A$ del otro aparato al recibir el tercer mensaje de autenticación de identidad se configura para:

verificar si el número aleatorio $N_A$ en el tercer mensaje de autenticación de identidad recibido es consistente con el último número aleatorio recibido $N_A$, y si no son consistentes, determinar que el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación;
verificar si el número aleatorio $N_B$ en el tercer mensaje de autenticación de identidad recibido es consistente con el número aleatorio $N_B$ transmitido por el aparato al otro aparato, y si no son consistentes, determinar que el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación; y
verificar $Sig_A$ usando una clave pública $CP_A$ del otro aparato verificar la legalidad del otro aparato, y si el otro aparato no es legal, determinar que el tercer mensaje de autenticación de identidad es incorrecto como resultado de la verificación, en el que la clave pública $CP_A$ del otro aparato está comprendida en el certificado $Cert_A$ del otro aparato;
en el que si uno cualquiera de los controles muestra incorrección, entonces se determina que el $N_A$ || $N_B$ || $Q_A$ || $Sig_A$ || $MacTag_A$ recibido es incorrecto como resultado de la verificación.

12. El procedimiento o aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 11, en el que el primer mensaje de autenticación de identidad se transmite después de ser encapsulado en una unidad de datos de protocolo ACT_REQ, el segundo mensaje de autenticación de identidad se transmite después de ser encapsulado en una unidad de datos del protocolo ACT_RES, el tercer mensaje de autenticación de identidad se transmite después de estar encapsulado en una unidad de datos de protocolo VFY_REQ, y el cuarto mensaje de autenticación de identidad se transmite después de estar encapsulado en una unidad de datos de protocolo VFY_RES, en el que ACT_REQ, ACT_RES, VFY_REQ y VFY_RES son formatos de unidades de datos de protocolo definidos de acuerdo con la norma ISO/IEC 13157-1.

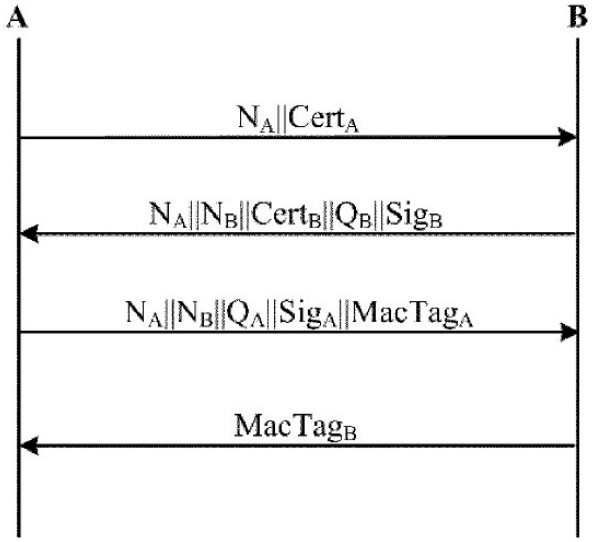


Fig.1

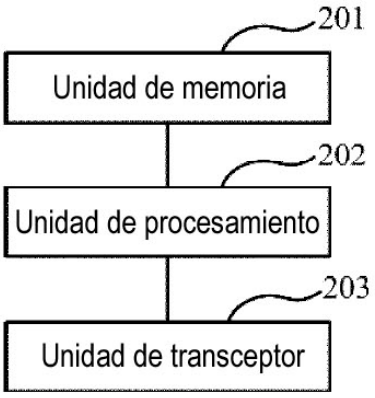


Fig.2

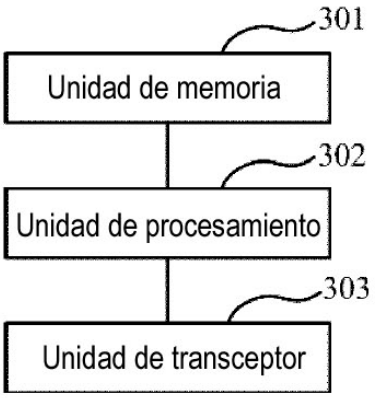


Fig.3