

MÉTODO DE CERTIFICACIÓN Y DISPOSITIVO RELACIONADO DEL MISMO

CAMPO DE LA INVENCION

Esta solicitud se refiere al campo de tecnologías de comunicación, y en particular, a un método
5 de certificación y un dispositivo relacionado del mismo.

ANTECEDENTES DE LA INVENCION

Un lado de red determina la seguridad de un lado de dispositivo terminal con base en una
tarjeta de módulo de identidad de abonado (subscriber identity module, SIM). El dispositivo
terminal se conoce brevemente como una terminal, o se conoce como equipo de usuario (user
10 equipment, UE). La lógica de seguridad básica es que la tarjeta de SIM y el lado de red
retienen conjuntamente una clave compartida, y un usuario realiza una operación en la clave
compartida en un proceso de acceso a la red, para realizar la autenticación y autorización.

Se puede enterar de que la verificación de seguridad de extremo a extremo entre una
red y el UE es una verificación desde un extremo de red hasta un extremo de tarjeta de SIM,
15 pero no se determina la confiabilidad de un dispositivo de hardware del UE.

BREVE DESCRIPCIÓN DE LA INVENCION

Esta solicitud proporciona un método de certificación y un dispositivo relacionado del mismo,
para realizar una certificación de confianza en una terminal.

De acuerdo con un primer aspecto, esta solicitud proporciona un método de
20 certificación. El método de certificación se aplica a un primer elemento de red. El primer
elemento de red es un elemento de red que tiene una capacidad de certificación de confianza.

El método de certificación incluye los siguientes pasos: El primer elemento de red
recibe la primera información de certificación de una terminal. El primer elemento de red
obtiene un primer resultado de certificación de confianza de la terminal con base en la primera
25 información de certificación y la primera información esperada.

En esta solución, el primer elemento de red obtiene el primer resultado de certificación
de confianza de la terminal con base en la primera información esperada y la primera
información de certificación de la terminal, para implementar la certificación de confianza de
la terminal, es decir, determinar si la terminal es confiable.

Con referencia a una posible implementación del primer aspecto, la primera información de certificación incluye un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación local al usar una clave simétrica, y la clave simétrica es una clave usada para certificación de confianza. La clave simétrica significa que la terminal y el primer elemento de red tienen una misma clave utilizada para la certificación de confianza.

Con referencia a una posible implementación del primer aspecto, la primera información esperada incluye un primer valor de verificación esperado. El primer valor de verificación esperado se obtiene al procesar el primer número aleatorio y la primera información de certificación esperada al usar la clave simétrica. La primera información de certificación esperada es un valor de referencia de la información de certificación local de la terminal.

En esta solicitud, el primer valor de verificación se obtiene al procesar el primer número aleatorio y la información de certificación local al usar la clave simétrica, tal que el primer elemento de red pueda verificar la confiabilidad de la terminal con base en el primer valor de verificación y el primer valor de verificación esperado. La terminal es confiable si el primer valor de verificación es el mismo que el primer valor de verificación esperado; o la terminal no es confiable si el primer valor de verificación es diferente del primer valor de verificación esperado.

Con referencia a una posible implementación del primer aspecto, la primera información de certificación incluye además la información de certificación local de la terminal.

Con referencia a una posible implementación del primer aspecto, la primera información esperada incluye además la primera información de certificación esperada.

En esta solicitud, cuando el primer valor de verificación es el mismo que el primer valor de verificación esperado, y la información de certificación local es la misma que la primera información de certificación esperada, el primer elemento de red puede determinar que la terminal es confiable; o cuando el primer valor de verificación es diferente del primer valor de verificación esperado, y/o la información de certificación local es diferente de la primera información de certificación esperada, el primer elemento de red determina que la terminal no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el primer valor de verificación y el primer valor de verificación esperado, y la información de certificación local y la primera información de certificación

esperada son las mismas, para garantizar una mayor fiabilidad de un resultado de certificación de confianza de la terminal.

Con referencia a una posible implementación del primer aspecto, antes de que el primer elemento de red reciba la primera información de certificación de la terminal, el método
5 incluye además: El primer elemento de red recibe una primera solicitud de certificación de un segundo elemento de red. La primera solicitud de certificación incluye información de identificación de la terminal. El primer elemento de red envía una segunda solicitud de certificación a la terminal. La segunda solicitud de certificación incluye el primer número aleatorio, y el primer número aleatorio corresponde a la información de identificación de la
10 terminal.

Por lo tanto, en esta solicitud, el primer elemento de red inicia la certificación de confianza de la terminal en respuesta a la primera solicitud de certificación enviada por el segundo elemento de red. Debido a que el primer número aleatorio corresponde a la información de identificación de la terminal, el primer elemento de red puede obtener el primer
15 número aleatorio con base en la información de identificación de la terminal. Entonces, el primer elemento de red envía la segunda solicitud de certificación a la terminal. La segunda solicitud de certificación incluye el primer número aleatorio. De esta manera, la terminal puede generar el primer valor de verificación con base en el primer número aleatorio y la información de certificación local.

20 Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además los siguientes pasos:

El primer elemento de red obtiene un primer vector de confianza que corresponde a la información de identificación de la terminal. El primer vector de confianza incluye la primera información esperada.

25 En esta solicitud, el primer elemento de red puede obtener el primer vector de confianza que corresponde a la información de identificación de la terminal con base en la información de identificación de la terminal, para obtener la primera información esperada.

Con referencia a una posible implementación del primer aspecto, una implementación específica en la que el primer elemento de red obtiene el primer vector de confianza que
30 corresponde a la información de identificación de la terminal incluye: El primer elemento de red envía una solicitud de vector de confianza a un tercer elemento de red. La solicitud de

vector de confianza incluye la información de identificación de la terminal. El primer elemento de red recibe el primer vector de confianza que corresponde a la información de identificación de la terminal y que se envía por el tercer elemento de red.

5 En esta solicitud, el primer elemento de red puede iniciar la solicitud de vector de confianza al tercer elemento de red, para obtener el primer vector de confianza. El tercer elemento de red puede obtener el primer vector de confianza con base en la información de identificación de la terminal.

10 Con referencia a una posible implementación del primer aspecto, otra implementación específica en la que el primer elemento de red obtiene el primer vector de confianza que corresponde a la información de identificación de la terminal incluye: El primer elemento de red recibe el primer vector de confianza de un elemento de red de autenticación.

En esta solicitud, el elemento de red de autenticación puede enviar el primer vector de confianza al primer elemento de red, tal que el primer elemento de red obtenga el primer vector de confianza.

15 Con referencia a una posible implementación del primer aspecto, el primer vector de confianza incluye además la clave simétrica. Por ejemplo, el primer elemento de red puede realizar la derivación de clave con base en la clave simétrica. Para otro ejemplo, el primer elemento de red puede reprocesar el primer número aleatorio y la primera información de certificación esperada por el uso de la clave simétrica, para obtener un nuevo valor de
20 verificación, y verificar el primer valor de verificación con base en el nuevo valor de verificación.

Con referencia a una posible implementación del primer aspecto, la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza;

25 una primera clave derivada, donde la primera clave derivada se deriva de la clave raíz utilizada para la certificación de confianza;

una segunda clave derivada, donde la segunda clave derivada se deriva de una clave raíz utilizada para la autenticación; y

30 una tercera clave derivada, donde la tercera clave derivada se deriva de una clave de autenticación, y la clave de autenticación se deriva de la clave raíz utilizada para la autenticación.

Cuando la clave simétrica es la segunda clave derivada o la tercera clave derivada, la terminal no necesita establecer la clave raíz utilizada para la certificación de confianza, y puede obtener la segunda clave derivada o la tercera clave derivada utilizando la clave raíz utilizada para la autenticación.

5 Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red realiza la derivación de clave con base en la clave simétrica, para obtener una cuarta clave derivada. La cuarta clave derivada es cualquiera de las siguientes: una primera clave de anclaje y la clave de autenticación.

10 Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red envía un segundo vector de confianza al segundo elemento de red o a un primer nodo. El segundo vector de confianza incluye la segunda información esperada, el segundo vector de confianza se utiliza por el segundo elemento de red o el primer nodo para realizar la certificación de confianza en
15 la terminal, y la segunda información esperada incluye un segundo valor de verificación esperado.

En esta solicitud, el primer elemento de red envía el segundo vector de confianza al segundo elemento de red o al primer nodo, tal que el segundo elemento de red o el primer nodo puedan realizar la certificación de confianza en la terminal con base en la segunda
20 información esperada, y desplegar la capacidad de certificación de confianza en el segundo elemento de red o el primer nodo. El primer nodo puede ser un dispositivo de red de acceso.

Por ejemplo, el segundo elemento de red o el primer nodo realiza la certificación de confianza con base en la segunda información de certificación de la terminal y la segunda información esperada. La segunda información de certificación incluye un segundo valor de verificación, el segundo valor de verificación se obtiene al procesar un segundo número aleatorio y la información de certificación local de la terminal por el uso de una quinta clave derivada, y la quinta clave derivada se deriva de la clave simétrica. El segundo valor de verificación esperado se obtiene al procesar el segundo número aleatorio y la segunda información de certificación esperada al usar la quinta clave derivada, y la segunda
25 información de certificación esperada es la misma que la primera información de certificación esperada. Cuando se realiza la certificación de confianza en la terminal, el segundo elemento de red o el primer nodo se pueden enterar, a través de la comparación, de si el segundo valor de verificación es el mismo que el segundo valor de verificación esperado. La terminal es
30

confiable si el segundo valor de verificación es el mismo que el segundo valor de verificación esperado; o la terminal no es confiable si el segundo valor de verificación es diferente del segundo valor de verificación esperado.

5 Con referencia a una posible implementación del primer aspecto, la segunda información esperada incluye además la segunda información de certificación esperada. Por ejemplo, la segunda información de certificación incluye además la información de certificación local de la terminal. En esta solicitud, cuando el segundo valor de verificación es el mismo que el segundo valor de verificación esperado, y la información de certificación local es la misma que la segunda información de certificación esperada, el segundo elemento de red o el primer nodo determina que la terminal es confiable; o cuando el segundo valor de verificación es diferente del segundo valor de verificación esperado, y/o la información de certificación local es diferente de la segunda información de certificación esperada, la terminal no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el segundo valor de verificación y el segundo valor de verificación esperado, y la información de certificación local y la segunda información de certificación esperada son las mismas, para garantizar una mayor fiabilidad del resultado de certificación de confianza de la terminal.

20 En esta solicitud, de manera similar al primer vector de confianza, el segundo vector de confianza puede incluir además la quinta clave derivada, tal que el segundo elemento de red o el primer nodo puedan usar la quinta clave derivada. Por ejemplo, el segundo elemento de red o el primer nodo pueden realizar la derivación de clave con base en la quinta clave derivada. Para otro ejemplo, el segundo elemento de red o el primer nodo pueden reprocesar el segundo número aleatorio y la segunda información de certificación esperada por el uso de la quinta clave derivada, para obtener un nuevo valor de verificación, y verificar el segundo valor de verificación con base en el nuevo valor de verificación.

Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red recibe el segundo vector de confianza del tercer elemento de red.

30 En esta solicitud, después de determinar el segundo vector de confianza, el tercer elemento de red puede enviar el segundo vector de confianza al primer elemento de red.

Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red envía un tercer

vector de confianza al segundo elemento de red o a un primer nodo. El tercer vector de confianza incluye una quinta clave derivada y segunda información de certificación esperada, el tercer vector de confianza se utiliza por el segundo elemento de red o el primer nodo para realizar la certificación de confianza en la terminal, y la quinta clave derivada se deriva de la clave simétrica.

En esta solicitud, se proporciona otro método para implementar la capacidad de certificación de confianza en el segundo elemento de red o el primer nodo. El primer elemento de red envía el tercer vector de confianza al segundo elemento de red o al primer nodo, el segundo elemento de red o el primer nodo genera el segundo número aleatorio que corresponde a la información de identificación de la terminal, y el segundo elemento de red o el primer nodo procesa el segundo número aleatorio y la segunda información de certificación esperada con base en la quinta clave derivada, para obtener el segundo valor de verificación esperado. El segundo elemento de red o el primer nodo pueden realizar la certificación de confianza de la terminal con base en el segundo valor de verificación esperado, o el segundo elemento de red o el primer nodo realiza la certificación de confianza de la terminal con base en la segunda información de certificación esperada y el segundo valor de verificación esperado, o el segundo elemento de red o el primer nodo realiza la certificación de confianza de la terminal con base en el segundo número aleatorio, la segunda información de certificación esperada, y el segundo valor de verificación esperado.

Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red recibe el tercer vector de confianza del tercer elemento de red.

En esta solicitud, después de determinar el tercer vector de confianza, el tercer elemento de red puede enviar el tercer vector de confianza al primer elemento de red.

Con referencia a una posible implementación del primer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red envía el primer resultado de certificación de confianza a la terminal.

En esta solicitud, el primer elemento de red retroalimenta un resultado de certificación de confianza de la terminal a la terminal, tal que la terminal obtenga el resultado de certificación de confianza de la terminal.

De acuerdo con un segundo aspecto, esta solicitud proporciona además un método de

certificación. El método se aplica a una terminal, y la terminal es un dispositivo que tiene un requisito de certificación de confianza.

El método de certificación incluye los siguientes pasos: La terminal determina la primera información de certificación. La terminal envía la primera información de certificación
5 a un primer elemento de red.

En esta solución, después de determinar la primera información de certificación, la terminal envía la primera información de certificación al primer elemento de red, tal que el primer elemento de red obtenga un primer resultado de certificación de confianza de la terminal con base en la primera información esperada y la primera información de certificación
10 de la terminal, para implementar la certificación de confianza de la terminal, es decir, determinar si la terminal es confiable.

Con referencia a una posible implementación del segundo aspecto, la primera información de certificación incluye un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación
15 local al usar una clave simétrica, y la clave simétrica es una clave usada para certificación de confianza. Por consiguiente, la primera información esperada incluye un primer valor de verificación esperado. El primer elemento de red puede verificar la confiabilidad de la terminal con base en el primer valor de verificación y el primer valor de verificación esperado. La terminal es confiable si el primer valor de verificación es el mismo que el primer valor de
20 verificación esperado; o la terminal no es confiable si el primer valor de verificación es diferente del primer valor de verificación esperado.

Con referencia a una posible implementación del segundo aspecto, la primera información de certificación incluye además la información de certificación local de la terminal. Por consiguiente, la primera información esperada incluye además la primera información de
25 certificación esperada.

En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el primer valor de verificación y el primer valor de verificación esperado, y la información de certificación local y la primera información de certificación esperada son las mismas, para garantizar una mayor fiabilidad de un resultado de certificación de confianza
30 de la terminal.

Con referencia a una posible implementación del segundo aspecto, antes de que la

terminal determine la primera información de certificación, el método de certificación incluye además: La terminal recibe una segunda solicitud de certificación del primer elemento de red. La segunda solicitud de certificación incluye el primer número aleatorio.

5 Con referencia a una posible implementación del segundo aspecto, la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza;

una primera clave derivada, donde la primera clave derivada se deriva de la clave raíz utilizada para la certificación de confianza;

10 una segunda clave derivada, donde la segunda clave derivada se deriva de una clave raíz utilizada para la autenticación; y

una tercera clave derivada, donde la tercera clave derivada se deriva de una clave de autenticación.

15 Con referencia a una posible implementación del segundo aspecto, el método de certificación incluye además el siguiente paso: La terminal recibe el primer resultado de certificación de confianza de la terminal del primer elemento de red. El primer resultado de certificación de confianza se obtiene con base en la primera información de certificación y la primera información esperada.

20 Con referencia a una posible implementación del segundo aspecto, el método de certificación incluye además el siguiente paso: La terminal envía la segunda información de certificación a un segundo elemento de red o a un primer nodo. De esta manera, el segundo elemento de red o el primer nodo pueden realizar la certificación de confianza de la terminal con base en la segunda información de certificación y la segunda información esperada.

25 De acuerdo con un tercer aspecto, esta solicitud proporciona además un método de certificación. El método de certificación se aplica a un primer elemento de red y un segundo elemento de red.

30 El método de certificación incluye los siguientes pasos: El segundo elemento de red envía una primera solicitud de certificación al primer elemento de red. La primera solicitud de certificación incluye información de identificación de una terminal. El primer elemento de red recibe la primera información de certificación de la terminal. El primer elemento de red obtiene un primer resultado de certificación de confianza de la terminal con base en la primera

información de certificación y la primera información esperada.

5 En esta solicitud, el primer elemento de red inicia la certificación de confianza de la terminal en respuesta a la primera solicitud de certificación enviada por el segundo elemento de red. Después de que el primer elemento de red recibe la primera información de certificación de la terminal, el primer elemento de red obtiene el primer resultado de certificación de confianza de la terminal con base en la primera información esperada y la primera información de certificación, para implementar la certificación de confianza de la terminal.

10 Con referencia a una posible implementación del tercer aspecto, la primera información de certificación incluye un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación local al usar una clave simétrica, y la clave simétrica es una clave usada para certificación de confianza. Por consiguiente, la primera información esperada incluye un primer valor de verificación esperado. En esta solicitud, el primer elemento de red puede verificar la confiabilidad de la terminal con
15 base en el primer valor de verificación y el primer valor de verificación esperado. La terminal es confiable si el primer valor de verificación es el mismo que el primer valor de verificación esperado; o la terminal no es confiable si el primer valor de verificación es diferente del primer valor de verificación esperado.

20 Con referencia a una posible implementación del tercer aspecto, la primera información de certificación incluye además la información de certificación local de la terminal. Por consiguiente, la primera información esperada incluye además la primera información de certificación esperada. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el primer valor de verificación y el primer valor de verificación esperado, y la información de certificación local y la primera información de
25 certificación esperada son las mismas, para garantizar una mayor fiabilidad de un resultado de certificación de confianza de la terminal.

30 Con referencia a una posible implementación del tercer aspecto, antes de que el primer elemento de red reciba la primera información de certificación de la terminal, el método de certificación incluye además el siguiente paso: El primer elemento de red envía una segunda solicitud de certificación a la terminal. La segunda solicitud de certificación incluye el primer número aleatorio, y el primer número aleatorio corresponde a la información de identificación de la terminal.

Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red obtiene un primer vector de confianza que corresponde a la información de identificación de la terminal. El primer vector de confianza incluye la primera información esperada.

- 5 Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además los siguientes pasos:

El primer elemento de red envía una solicitud de vector de confianza a un tercer elemento de red. La solicitud de vector de confianza incluye la información de identificación de la terminal.

- 10 El tercer elemento de red envía el primer vector de confianza que corresponde a la información de identificación de la terminal al primer elemento de red.

Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además el siguiente paso: El primer elemento de red recibe el primer vector de confianza de un elemento de red de autenticación.

- 15 Con referencia a una posible implementación del tercer aspecto, la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza;

una primera clave derivada, donde la primera clave derivada se deriva de la clave raíz utilizada para la certificación de confianza;

- 20 una segunda clave derivada, donde la segunda clave derivada se deriva de una clave raíz utilizada para la autenticación; y

una tercera clave derivada, donde la tercera clave derivada se deriva de una clave de autenticación.

- 25 Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además: El primer elemento de red realiza la derivación de clave con base en la clave simétrica, para obtener una cuarta clave derivada. La cuarta clave derivada es cualquiera de las siguientes: una primera clave de anclaje y la clave de autenticación.

Con referencia a una posible implementación del tercer aspecto, el método de

certificación incluye además: El primer elemento de red envía un segundo vector de confianza al segundo elemento de red o a un primer nodo. El segundo vector de confianza incluye la segunda información esperada, el segundo vector de confianza se utiliza por el segundo elemento de red o el primer nodo para realizar la certificación de confianza en la terminal, y la
5 segunda información esperada incluye un segundo valor de verificación esperado.

Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además: El tercer elemento de red envía un segundo vector de confianza al primer elemento de red.

Con referencia a una posible implementación del tercer aspecto, el método de
10 certificación incluye además: El primer elemento de red envía un tercer vector de confianza al segundo elemento de red o a un primer nodo. El tercer vector de confianza incluye una quinta clave derivada y segunda información de certificación esperada, el tercer vector de confianza se utiliza por el segundo elemento de red o el primer nodo para realizar la certificación de confianza en la terminal, y la quinta clave derivada se deriva de la clave simétrica. El segundo
15 elemento de red o el primer nodo obtiene un segundo número aleatorio. El segundo elemento de red o el primer nodo obtiene el segundo valor de verificación esperado con base en la quinta clave derivada, el segundo número aleatorio, y la segunda información de certificación esperada.

Con referencia a una posible implementación del tercer aspecto, el método de
20 certificación incluye además: El tercer elemento de red envía el tercer vector de confianza al primer elemento de red.

Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además: El segundo elemento de red o el primer nodo recibe la segunda información de certificación de la terminal. El segundo elemento de red o el primer nodo
25 obtiene un segundo resultado de certificación de confianza de la terminal con base en la segunda información de certificación y la segunda información esperada.

Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además: El segundo elemento de red o el primer nodo envía el segundo resultado de certificación de confianza a la terminal.

30 Con referencia a una posible implementación del tercer aspecto, el método de certificación incluye además: El primer elemento de red envía el primer resultado de

certificación de confianza a la terminal.

De acuerdo con un cuarto aspecto, esta solicitud proporciona además un método de certificación. El método se aplica a un segundo nodo.

El método de certificación incluye los siguientes pasos: El segundo nodo envía una
5 tercera solicitud de certificación a un tercer nodo. El segundo nodo recibe la tercera información de certificación del tercer nodo. El segundo nodo obtiene un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

En esta solución, el segundo nodo inicia la certificación de confianza del tercer nodo,
10 y realiza la certificación de confianza en el tercer nodo con base en la tercera información esperada y la tercera información de certificación del tercer nodo, para obtener el resultado de la certificación de confianza del tercer nodo, es decir, determina si el tercer nodo es confiable.

Con referencia a una posible implementación del cuarto aspecto, la tercera información
15 de certificación incluye un tercer valor de verificación, el tercer valor de verificación se obtiene al procesar un tercer número aleatorio e información de certificación local por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza.

Con referencia a una posible implementación del cuarto aspecto, la tercera información
esperada incluye un tercer valor de verificación esperado. En esta solicitud, cuando se realiza
20 la certificación de confianza en el tercer nodo, el segundo nodo se puede enterar a través de la comparación, de si el tercer valor de verificación es el mismo que el tercer valor de verificación esperado. El tercer nodo es confiable si el tercer valor de verificación es el mismo que el tercer valor de verificación esperado; o el tercer nodo no es confiable si el tercer valor de verificación es diferente del tercer valor de verificación esperado.

Con referencia a una posible implementación del cuarto aspecto, la tercera información
25 de certificación incluye además información de certificación local del tercer nodo.

Con referencia a una posible implementación del cuarto aspecto, la tercera información
esperada incluye además la tercera información de certificación esperada.

En esta solicitud, cuando el tercer valor de verificación es el mismo que el tercer valor
30 de verificación esperado, y la información de certificación local del tercer nodo es la misma

que la tercera información de certificación esperada, el segundo nodo determina que el tercer nodo es confiable; o cuando el tercer valor de verificación es diferente del tercer valor de verificación esperado, y/o la información de certificación local del tercer nodo es diferente de la tercera información de certificación esperada, el tercer nodo no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el tercer valor de verificación y el tercer valor de verificación esperado, y la información de certificación local del tercer nodo y la tercera información de certificación esperada son las mismas, para garantizar una mayor fiabilidad del resultado de certificación de confianza del tercer nodo.

10 Con referencia a una posible implementación del cuarto aspecto, el método de certificación incluye además los siguientes pasos: El segundo nodo envía una solicitud de vector de confianza a un tercer elemento de red. La solicitud de vector de confianza incluye información de identificación del tercer nodo. El segundo nodo recibe un cuarto vector de confianza del tercer elemento de red. El cuarto vector de confianza incluye la tercera información esperada.

En esta solución, el tercer elemento de red recibe la solicitud del segundo nodo, genera el cuarto vector de confianza, y retorna el cuarto vector de confianza al segundo nodo, tal que el segundo nodo obtenga la tercera información esperada.

20 Con referencia a una posible implementación del cuarto aspecto, la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza; y

una sexta clave derivada, donde la sexta clave derivada se deriva de la clave raíz utilizada para la certificación de confianza.

25 Con referencia a una posible implementación del cuarto aspecto, el método de certificación incluye además: El segundo nodo envía el resultado de certificación de confianza al tercer nodo.

De acuerdo con un quinto aspecto, esta solicitud proporciona además un método de certificación. El método se aplica a un tercer nodo.

30 El método de certificación incluye los siguientes pasos: El tercer nodo recibe una tercera solicitud de certificación de un segundo nodo. El tercer nodo envía la tercera

información de certificación al segundo nodo. La tercera información de certificación incluye un tercer valor de verificación, el tercer valor de verificación se obtiene al procesar un tercer número aleatorio e información de certificación local por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza.

5 En esta solución, el tercer nodo envía la tercera información de certificación al segundo nodo en respuesta a la tercera solicitud de certificación, tal que el segundo nodo realice la certificación de confianza en el tercer nodo con base en la tercera información esperada y la tercera información de certificación, para obtener un resultado de certificación de confianza del tercer nodo.

10 Con referencia a una posible implementación del quinto aspecto, la tercera información esperada incluye un tercer valor de verificación esperado. El segundo nodo puede verificar la confiabilidad del tercer nodo con base en el tercer valor de verificación y el tercer valor de verificación esperado. El tercer nodo es confiable si el tercer valor de verificación es el mismo que el tercer valor de verificación esperado; o el tercer nodo no es confiable si el tercer valor
15 de verificación es diferente del tercer valor de verificación esperado.

 Con referencia a una posible implementación del quinto aspecto, la tercera información de certificación incluye además información de certificación local del tercer nodo. Por consiguiente, la tercera información esperada incluye además la tercera información de certificación esperada. Cuando el tercer valor de verificación es el mismo que el tercer valor
20 de verificación esperado, y la información de certificación local del tercer nodo es la misma que la tercera información de certificación esperada, el segundo nodo puede determinar que el tercer nodo es confiable; o cuando el tercer valor de verificación es diferente del tercer valor de verificación esperado, y/o la información de certificación local del tercer nodo es diferente de la tercera información de certificación esperada, se determina que el tercer nodo no es
25 confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el tercer valor de verificación y el tercer valor de verificación esperado, y la información de certificación local del tercer nodo y la tercera información de certificación esperada son las mismas, para garantizar una mayor fiabilidad del resultado de certificación de confianza del tercer nodo.

30 Con referencia a una posible implementación del quinto aspecto, la clave simétrica es cualquiera de las siguientes:

 una clave raíz utilizada para la certificación de confianza; y

una sexta clave derivada, donde la sexta clave derivada se deriva de la clave raíz utilizada para la certificación de confianza.

5 Con referencia a una posible implementación del quinto aspecto, el método de certificación incluye además: El tercer nodo recibe un resultado de certificación de confianza del tercer nodo desde el segundo nodo. El resultado de la certificación de confianza se obtiene con base en la tercera información de certificación y la tercera información esperada.

De acuerdo con un sexto aspecto, esta solicitud proporciona además un método de certificación. El método se aplica a un segundo nodo y un tercer nodo.

10 El método de certificación incluye los siguientes pasos: El segundo nodo envía una tercera solicitud de certificación al tercer nodo. El tercer nodo envía la tercera información de certificación al segundo nodo. El segundo nodo obtiene un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

15 Con referencia a una posible implementación del sexto aspecto, la tercera información de certificación incluye un tercer valor de verificación, el tercer valor de verificación se obtiene al procesar un tercer número aleatorio e información de certificación local por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza. Por consiguiente, la tercera información esperada incluye un tercer valor de verificación esperado. El segundo nodo puede verificar la confiabilidad del tercer nodo con base en el
20 tercer valor de verificación y el tercer valor de verificación esperado. El tercer nodo es confiable si el tercer valor de verificación es el mismo que el tercer valor de verificación esperado; o el tercer nodo no es confiable si el tercer valor de verificación es diferente del tercer valor de verificación esperado.

25 Con referencia a una posible implementación del sexto aspecto, la tercera información de certificación incluye además información de certificación local del tercer nodo. Por consiguiente, la tercera información esperada incluye además la tercera información de certificación esperada. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el tercer valor de verificación y el tercer valor de verificación esperado, y la información de certificación local del tercer nodo y la tercera
30 información de certificación esperada son las mismas, para garantizar una mayor fiabilidad del resultado de certificación de confianza del tercer nodo.

Con referencia a una posible implementación del sexto aspecto, el método de certificación incluye además los siguientes pasos: El segundo nodo envía una solicitud de vector de confianza a un tercer elemento de red. La solicitud de vector de confianza incluye información de identificación del tercer nodo. El tercer elemento de red envía un cuarto vector de confianza al segundo nodo. El cuarto vector de confianza incluye la tercera información esperada.

Con referencia a una posible implementación del sexto aspecto, la clave simétrica es cualquiera de las siguientes:

- una clave raíz utilizada para la certificación de confianza; y
- una sexta clave derivada, donde la sexta clave derivada se deriva de la clave raíz utilizada para la certificación de confianza.

Con referencia a una posible implementación del sexto aspecto, el método de certificación incluye además: El tercer nodo recibe un resultado de certificación de confianza del segundo nodo.

- De acuerdo con un séptimo aspecto, esta solicitud proporciona además un primer elemento de red, que incluye un módulo de recepción y un módulo de procesamiento.

El módulo de recepción se configura para recibir la primera información de certificación de una terminal.

- El módulo de procesamiento se configura para obtener un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación y la primera información esperada.

De acuerdo con un octavo aspecto, esta solicitud proporciona además una terminal, que incluye un módulo de determinación y un módulo de envío.

- El módulo de determinación se configura para determinar la primera información de certificación.

El módulo de envío se configura para enviar la primera información de certificación a un primer elemento de red.

De acuerdo con un noveno aspecto, esta aplicación proporciona además un sistema

de comunicación. El sistema incluye un primer elemento de red y un segundo elemento de red.

5 El segundo elemento de red se configura para enviar una primera solicitud de certificación al primer elemento de red. La primera solicitud de certificación incluye información de identificación de una terminal.

El primer elemento de red se configura para recibir la primera información de certificación de la terminal.

10 El primer elemento de red se configura además para obtener un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación y la primera información esperada.

De acuerdo con un décimo aspecto, esta solicitud proporciona además un segundo nodo, que incluye un módulo de envío, un módulo de recepción, y un módulo de determinación.

El módulo de envío se configura para enviar una tercera solicitud de certificación a un tercer nodo.

15 El módulo de recepción se configura para recibir tercera información de certificación del tercer nodo.

El módulo de determinación se configura para obtener un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

20 De acuerdo con un undécimo aspecto, esta solicitud proporciona además un tercer nodo, que incluye un módulo de recepción y un módulo de envío.

El módulo de recepción se configura para recibir una tercera solicitud de certificación de un segundo nodo.

25 El módulo de envío se configura para enviar la tercera información de certificación al segundo nodo. La tercera información de certificación incluye un tercer valor de verificación, el tercer valor de verificación se obtiene al procesar un tercer número aleatorio e información de certificación local del tercer nodo por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza.

De acuerdo con un duodécimo aspecto, esta solicitud proporciona además un sistema de comunicación. El sistema incluye un segundo nodo y un tercer nodo.

El segundo nodo se configura para enviar una tercera solicitud de certificación al tercer nodo.

- 5 El tercer nodo se configura para enviar la tercera información de certificación al segundo nodo.

El segundo nodo se configura además para obtener un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

- 10 De acuerdo con un decimotercer aspecto, esta solicitud proporciona además un aparato de comunicación. El aparato de comunicación incluye uno o más procesadores y una o más memorias. La una o más memorias se acoplan al uno o más procesadores, la una o más memorias se configuran para almacenar código de programa de computadora, el código de programa de computadora incluye instrucciones de computadora, y cuando el uno o más
15 procesadores ejecutan las instrucciones de computadora, el aparato de comunicación se habilita para realizar el método de acuerdo con cualquiera del primer aspecto al sexto aspecto.

- De acuerdo con un decimocuarto aspecto, esta solicitud proporciona además un medio de almacenamiento leíble por computadora. El medio de almacenamiento leíble por computadora almacena instrucciones, y cuando las instrucciones se ejecutan por un
20 procesador, se implementa el método de acuerdo con cualquiera del primer aspecto al sexto aspecto.

- De acuerdo con un decimoquinto aspecto, esta solicitud proporciona además un producto de programa de computadora, que incluye un programa de computadora. Cuando el programa de computadora se ejecuta en un procesador, se implementa el método de acuerdo
25 con cualquiera del primer aspecto al sexto aspecto.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La figura 1 es un diagrama de una estructura de una arquitectura de sistema de certificación de acuerdo con una modalidad de esta solicitud;

- La figura 2A es un diagrama de una arquitectura de red de acuerdo con una modalidad
30 de esta solicitud;

La figura 2B es un diagrama de otra arquitectura de red de acuerdo con una modalidad de esta solicitud;

La figura 2C es un diagrama de un procedimiento de autenticación de acuerdo con una modalidad de esta solicitud;

5 La figura 3 es un diagrama de flujo de un método de certificación de acuerdo con una modalidad de esta solicitud;

La figura 4A es un diagrama de un procedimiento de certificación de confianza de acuerdo con una modalidad de esta solicitud;

10 La figura 4B es un diagrama de una arquitectura de clave de acuerdo con una modalidad de esta solicitud;

La figura 4C es un diagrama de flujo de interacción de un método de certificación de acuerdo con una modalidad de esta solicitud;

La figura 4D es un diagrama de otra arquitectura de clave de acuerdo con una modalidad de esta solicitud;

15 La figura 4E es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud;

La figura 4F es un diagrama de otra arquitectura de clave de acuerdo con una modalidad de esta solicitud;

20 La figura 4G es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud;

La figura 4H es un diagrama de otra arquitectura de clave de acuerdo con una modalidad de esta solicitud;

La figura 4I es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud;

25 La figura 4J es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud;

La figura 4K es un diagrama de flujo de interacción de otro método de certificación de

acuerdo con una modalidad de esta solicitud;

La figura 5 es un diagrama de flujo de otro método de certificación de acuerdo con una modalidad de esta solicitud;

5 La figura 6A es un diagrama de otro procedimiento de certificación de confianza de acuerdo con una modalidad de esta solicitud;

La figura 6B es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud;

La figura 7 es un diagrama de una estructura de un primer elemento de red de acuerdo con una modalidad de esta solicitud;

10 La figura 8 es un diagrama de una estructura de una terminal de acuerdo con una modalidad de esta solicitud;

La figura 9 es un diagrama de una estructura de un segundo nodo de acuerdo con una modalidad de esta solicitud;

15 La figura 10 es un diagrama de una estructura de un tercer nodo de acuerdo con una modalidad de esta solicitud; y

La figura 11 es un diagrama de una estructura de un aparato de comunicación de acuerdo con una modalidad de la presente solicitud.

DESCRIPCIÓN DETALLADA DE LA INVENCION

20 Se propone simplemente que los términos utilizados en las siguientes modalidades de esta solicitud describan modalidades específicas, pero no se propone que limiten esta solicitud. Las expresiones singulares "uno", "un tipo de", "el", "lo anterior", "eso", y "esto" utilizadas en la especificación y las reivindicaciones anexas de esta solicitud también se propone que incluyan expresiones plurales, salvo que se especifique lo contrario en el contexto claramente. Se debe entender además que, el término "y/o" utilizado en esta solicitud indica e incluye una
25 cualquiera o todas las combinaciones posibles de uno o más artículos listados.

Los términos "primero" y "segundo" mencionados a continuación se proponen simplemente para un propósito de descripción, y no se entenderán como una indicación o implicación de importancia relativa o indicación implícita de una cantidad de características

técnicas indicadas. Por lo tanto, una característica limitada por "primero" y "segundo" puede incluir de manera explícita o implícitamente una o más características. En las descripciones de las modalidades de esta solicitud, salvo que se especifique lo contrario, "una pluralidad de" significa dos o más.

- 5 Debido a que las modalidades de esta solicitud se relacionan con un método, para facilitar la comprensión, lo siguiente describe primero los términos y conceptos relacionados en las modalidades de esta solicitud.

(1) Informática de confianza

10 La informática de confianza (Trust Computing, TC) es una tecnología que permite que una computadora se ejecute de la manera esperada. "de confianza" enfatiza que un resultado de comportamiento es predecible y controlable. La informática de confianza se aplica por hardware y software de computadora. Una tecnología de confianza para un sistema informático comienza con una raíz de confianza y evoluciona para confiar en una plataforma de hardware, un sistema operativo, y una aplicación. La fuerza de gestión y autenticación de
15 cada capa corresponde a la confiabilidad de cada capa. Además, la confianza se extiende al sistema de computadora completo, y se toman medidas de protección para garantizar la integridad de los recursos de computadora y los comportamientos de computadora esperados, para mejorar la confiabilidad del sistema de computadora.

20 La informática de confianza incluye dos direcciones de investigación diferentes. Una dirección de investigación es garantizar la confiabilidad de una base informática de confianza (Trust Computing Base, TCB) por el uso de un dispositivo antimanipulación física, y construir un sistema informático de confianza del sistema informático por el uso de la TCB como un anclaje de confianza. El dispositivo antimanipulación física es, por ejemplo, un módulo de plataforma de confianza (trusted platform module, TPM), y el TPM es un chip construido dentro
25 de una computadora para proporcionar una raíz de confianza para la computadora. La otra dirección de investigación es construir un sistema informático aislado para garantizar la confiabilidad de un entorno de ejecución de código de software sensible específico. La evolución es con base en esta idea, para desarrollar un entorno de ejecución de confianza universal (Trust Execution Environment, TEE) con base en un modo de seguridad especial de
30 una unidad de procesamiento central (Central Processing Unit, CPU).

Un tipo de informática de confianza incluye, pero no se limita a, uno o más de un TPM, un módulo de criptografía de confianza (trusted cryptography module, TCM), extensiones de

protección de software de Intel (Intel software guard extensions, Intel SGX) y una zona de confianza (trustedzone).

(2) Tecnología de certificación de confianza

En la tecnología de certificación de confianza, se verifica un valor de certificación de hardware y software de un dispositivo, para garantizar que el dispositivo no se manipule por un atacante. La figura 1 muestra una arquitectura de sistema de certificación. La arquitectura incluye un endosante (endorser), un proveedor de valor de referencia (reference value provider), un certificador (attester), un verificador (verifier), y una parte que depende (relying party). El endosante, el proveedor de valor de referencia, y el certificador proporcionan al verificador con la información utilizada para generar un resultado de certificación de confianza. El endosante proporciona un endoso de certificador (attester endorsements), es decir, un certificado de raíz de confianza. El certificado de raíz de confianza se utiliza para determinar que un chip de seguridad en el certificador es confiable, y el certificado incluye una clave pública. El proveedor de valores de referencia proporciona un valor de referencia de información de certificación, es decir, información de certificación esperada. El valor de referencia de información de certificación es un valor de referencia de la información de certificación local del certificador. El certificador proporciona la información de certificación local (evidencia) al verificador.

El certificador es un dispositivo equipado con una función de informática de confianza. En una tecnología informática de confianza, se utiliza un TPM como un ejemplo. Cuando se inicia el dispositivo, un chip de TPM en el dispositivo obtiene valores de medición en un sistema y software del sistema, y almacena de manera segura los valores de medición (es decir, información de certificación local) en un registro de configuración de plataforma (platform configuration register, PCR) del dispositivo.

Cuando se realiza la verificación de certificación de confianza en el certificador, el verificador primero propone un valor de desafío (por ejemplo, un número aleatorio) al certificador. Cuando el certificador recibe una solicitud, el chip de TPM calcula un resumen de la información de certificación local y el valor de desafío, y entonces firma el resumen al utilizar una clave privada del chip de TPM. El certificador envía una firma, la información de certificación local, y un certificado digital del certificador al verificador.

Después de recibir la firma, la información de certificación local y el certificado digital del certificador, el verificador verifica dos cosas: 1. Se verifica la autenticidad de la identidad

del certificador, para verificar si el certificado digital enviado por el certificador es un certificado proporcionado por un fabricante de TPM autorizado para el TPM. 2. Se verifica la información de certificación de confianza. Se comparan la información de certificación local y el valor de referencia de información de certificación, para verificar si la información de certificación local y el valor de referencia de información de certificación son iguales. La verificación tiene éxito si la información de certificación local y el valor de referencia de información de certificación son los mismos. Si ambas de las dos verificaciones anteriores son exitosas, el verificador puede reportar un resultado de certificación del certificador a la parte que depende (relying party). Además, después de que la verificación tenga éxito, el verificador puede realizar la derivación de claves por el uso de la clave pública.

Con referencia a los términos anteriores, lo siguiente describe un método en algunas modalidades y un método en modalidades de esta solicitud.

El método en las modalidades de esta solicitud puede aplicarse a una red de comunicación futura, tal como un sistema de evolución a largo plazo (Long Term Evolution, LTE), un sistema de comunicación móvil de evolución avanzada a largo plazo (Long Term Evolution-Advanced, LTE-A), una tecnología de evolución avanzada a largo plazo mejorada (Enhanced Long Term Evolution-Advanced, eLTE), un sistema de nueva radio (New Radio, NR) en un sistema de comunicación móvil de 5ª generación (5th Generation, 5G), o un sistema de comunicación móvil de 6ª generación (6th Generation, 6G), o se puede extender a un sistema de comunicación inalámbrica similar, tal como un sistema celular con relación a la fidelidad inalámbrica (Wireless Fidelity, Wi-Fi), interoperabilidad mundial para acceso de microondas (Worldwide Interoperability for Microwave Access, WiMAX), y un proyecto de asociación de 3ª generación (3rd Generation Partnership Project, 3GPP).

La figura 2A muestra una arquitectura de red aplicada a una modalidad de esta solicitud. Un sistema de comunicación móvil 5G se utiliza como un ejemplo para describir por separado todos los elementos de red que se pueden utilizar en la arquitectura de red.

1. Un dispositivo terminal se conoce brevemente como una terminal, y también se conoce como equipo de usuario (user equipment, UE). El dispositivo terminal puede incluir varios dispositivos de mano, dispositivos montados en el vehículo, dispositivos portátiles o dispositivos de cómputo que tienen una función de comunicación inalámbrica, otro dispositivo de procesamiento conectado a un módem inalámbrico, varias formas de terminales, una estación móvil (mobile station, MS), una terminal (terminal), una terminal de software, una terminal de acceso, una unidad de abonado (subscriber unit), una estación de dispositivo

terminal, una estación móvil (mobile station, MS), una estación remota, una terminal remota, un dispositivo móvil, un programa sustituto de dispositivo terminal, un aparato de dispositivo terminal, y similares. Por ejemplo, el dispositivo terminal puede ser un medidor de agua, un medidor de electricidad, o un sensor.

5 2. Una red de acceso de radio (radio access network, RAN) es una red que incluye una pluralidad de nodos de RAN, y puede implementar una función de capa física de radio, una función de programación de recursos y gestión de recursos de radio, una función de control de acceso de radio y una función de gestión de movilidad. La RAN se conecta a un elemento de red de plano de usuario a través de una interfaz de plano de usuario N3, para
10 transmitir datos de un dispositivo terminal. La RAN establece una conexión de señalización de plano de control a un elemento de red de gestión de acceso y movilidad a través de una interfaz de plano de control N2, para implementar una función tal como el control de portadora de acceso de radio.

 Específicamente, se puede proporcionar una función de acceso a red para un
15 dispositivo terminal autorizado en un área específica, y se pueden usar túneles de transmisión con diferente calidad con base en un nivel del dispositivo terminal, un requisito de servicio, y similares.

 La RAN puede gestionar un recurso de radio, y proporcionar un servicio de acceso para el dispositivo terminal, para completar adicionalmente el reenvío de una señal de control
20 y datos del dispositivo terminal entre el dispositivo terminal y una red de núcleo.

 La red de acceso de radio puede tener cualquiera de las siguientes palabras de reemplazo: un dispositivo de red de acceso y una red de acceso (access network, AN). El dispositivo de red de acceso puede ser una estación base, un NodoB evolucionado continuamente (gNB), un NodoB evolucionado (evolved NodeB, eNB), un punto de recepción
25 de transmisión (transmission reception point, TRP), un nodo de unidad central (central unit, CU), un nodo de unidad distribuida (distributed unit, DU), un punto de transmisión (transmission point, TP), un punto de recepción (receiving point, RP), y similares. Esto no se limita en la presente. En esta solicitud, la red de acceso de radio se describe por el uso del dispositivo de red de acceso como un ejemplo, y una función realizada por el dispositivo de
30 red de acceso también es aplicable a otra palabra de reemplazo de la red de acceso de radio.

 3. Un elemento de red de función de gestión de acceso y movilidad se configura principalmente para gestión de movilidad, gestión de acceso, y similares.

En un sistema de comunicación de 5G, el elemento de red de función de gestión de acceso y movilidad puede ser un elemento de red de función de gestión de acceso y movilidad (access and mobility management function, AMF). En un sistema de comunicación futuro, el elemento de red de función de gestión de acceso y movilidad puede seguir siendo un elemento de red de AMF, o puede tener otro nombre. Esto no se limita en esta solicitud.

La AMF es principalmente responsable de funciones tal como la autenticación de UE, la gestión de movilidad de UE, la selección del segmento de red y la selección de elemento de red de gestión de sesión; sirve como un anclaje de una conexión de señalización N1 y N2 y proporciona el encaminamiento de un mensaje de gestión de sesión N1/N2 (session management, SM) para un elemento de red de gestión de sesión; y mantiene y gestiona la información de estado del UE.

4. Un elemento de red de gestión de sesión se configura principalmente para gestión de sesión, asignación de dirección de protocolo de Internet (internet protocol, IP) y gestión de un dispositivo terminal, selección de una función de plano de usuario gestionable, un punto de terminación de una interfaz de función de control de política y facturación, una notificación de datos de enlace descendente, y similares.

En un sistema de comunicación de 5G, el elemento de red de gestión de sesión puede ser un elemento de red de función de gestión de sesión (session management function, SMF). En un sistema de comunicación futuro, el elemento de red de gestión de sesión puede seguir siendo un elemento de red de SMF, o puede tener otro nombre. Esto no se limita en esta solicitud.

La SMF es principalmente responsable de todas las funciones de plano de control de gestión de sesión de UE, incluyendo selección de elemento de red de plano de usuario, asignación de dirección de IP, gestión de QoS de sesión, obtención de información de control de política y facturación (policy and charging control, PCC) (de un elemento de red de control de política), y similares.

5. Un elemento de red de plano de usuario se configura para encaminamiento y reenvío de paquetes, procesamiento de calidad de servicio (quality of service, QoS) de datos de plano de usuario, y similares.

En un sistema de comunicación de 5G, el elemento de red de plano de usuario puede ser un elemento de red de función de plano de usuario (user plane function, UPF). En un

sistema de comunicación futuro, el elemento de red de plano de usuario puede seguir siendo un elemento de red de UPF, o puede tener otro nombre. Esto no se limita en esta solicitud.

La UPF proporciona principalmente una función de procesamiento de servicio de un plano de usuario. Como un punto de anclaje de una conexión de sesión de unidad de datos de protocolo (unidad de datos de protocolo, PDU), la UPF es responsable del filtrado de paquetes de datos, encaminamiento de servicio, reenvío de paquetes, una función de anclaje, control de velocidad, generación de información de facturación, mapeo y ejecución de QoS, identificación y encaminamiento de un identificador de enlace ascendente a una red de datos, activación de notificación de almacenamiento temporal de paquetes de enlace descendente y llegada de datos de enlace descendente, una conexión a una red de datos externa, y similares de equipo de usuario.

6. Un elemento de red de gestión de datos se configura para procesar un identificador de dispositivo terminal, autenticación de acceso, registro, gestión de movilidad, y similares.

En un sistema de comunicación de 5G, el elemento de red de gestión de datos puede ser un elemento de red de gestión de datos unificada (unified data management, UDM). En un sistema de comunicación futuro, el elemento de red de gestión de datos puede seguir siendo un elemento de red de UDM, o puede tener otro nombre. Esto no se limita en esta solicitud.

El elemento de red de UDM gestiona y controla principalmente los datos de usuario, por ejemplo, gestiona la información de suscripción, que incluye: obtener información de suscripción de un repositorio de datos y proporcionar la información de suscripción a otro elemento de red (por ejemplo, una AMF); generar una credencial de autenticación de 3GPP para el UE; y registrar y mantener un elemento de red (por ejemplo, una AMF representada por un ID de AMF 1 es una AMF de servicio actual del UE) que actualmente sirve al UE.

7. Un repositorio de datos se configura para almacenar datos de usuario.

En un sistema de comunicación de 5G, el repositorio de datos puede ser un repositorio de datos unificado (Unified Data Repository, UDR). En un sistema de comunicación futuro, el repositorio de datos puede seguir siendo un UDR, o puede tener otro nombre. Esto no se limita en esta solicitud.

El UDR se configura principalmente para almacenar datos de usuario, incluyendo datos de suscripción invocados por un elemento de red de gestión de datos, información de

política invocada por un elemento de red de control de política, datos estructurados usados para exposición de capacidad, y datos de aplicación invocados por un elemento de red de función de exposición de capacidad de red (network exposure function, NEF).

- 5 8. Un elemento de red de función de exposición de capacidad de red se configura para la conexión e interacción entre otro elemento de red interno de una red de núcleo y un servidor de aplicación externo de la red de núcleo, para proporcionar información de capacidad de red al servidor de aplicación externo, o proporcionar información sobre el servidor de aplicación externo a un elemento de red de núcleo.

10 En un sistema de comunicación de 5G, el elemento de red de exposición de capacidad de red puede ser un elemento de red de NEF. En un sistema de comunicación futuro, el elemento de red de exposición de capacidad de red puede seguir siendo una NEF, o puede tener otro nombre. Esto no se limita en esta solicitud.

- 15 9. Un elemento de red de servicio de aplicación interactúa con un elemento de red de núcleo para proporcionar algunos servicios, por ejemplo, interactúa con un elemento de red de control de política para realizar control de política de servicio, interactúa con un elemento de red de exposición de capacidad de red para obtener alguna información de capacidad de red o proporcionar alguna información de aplicación a una red, y proporciona alguna información de punto de acceso de red de datos al elemento de red de control de política para generar información de encaminamiento de un servicio de datos correspondiente.

20 En un sistema de comunicación de 5G, el elemento de red de servicio de aplicación puede ser un elemento de red de función de aplicación (Application Function, AF). En un sistema de comunicación futuro, el elemento de red de servicio de aplicación puede seguir siendo un elemento de red de AF, o puede tener otro nombre. Esto no se limita en esta solicitud. Por ejemplo, el elemento de red de servicio de aplicación puede tener cualquiera de
25 las siguientes palabras de reemplazo: un servidor de aplicación (application server, AS), un AF, un tercero, una aplicación de tercero, una aplicación de detección, un cliente de detección, una aplicación (application, APP), una aplicación de transmisión libre (over the top, OTT), y similares. OTT significa proporcionar varios servicios de aplicación para un usuario a través de Internet. La aplicación de OTT es una aplicación de capa superior de una red portadora,
30 por ejemplo, WeChat, Alipay, y Youku.

10. Un elemento de red de servicio de autenticación se configura para realizar autenticación de seguridad en UE cuando el UE accede a una red.

En un sistema de comunicación de 5G, el elemento de red de servicio de autenticación puede ser un elemento de red de función de servidor de autenticación (authentication server function, AUSF). En un sistema de comunicación futuro, el elemento de red de servicio de autenticación puede seguir siendo un elemento de red de AUSF, o puede tener otro nombre.

5 Esto no se limita en esta solicitud. Además, en esta modalidad, el elemento de red de servicio de autenticación también se puede entender como un elemento de red de autenticación.

El sistema de comunicación de 5G se utiliza como un ejemplo. Por ejemplo, la AUSF recibe una solicitud de una AMF para realizar la autenticación de identidad en el UE, solicita una clave de un UDM, y reenvía, a la AMF para el procesamiento de autenticación, la clave
10 entregada por el UDM.

11. El elemento de red de selección de segmento de red se configura para: seleccionar un conjunto de instancias de segmento para UE, y determinar un conjunto de AMF y NSSAI permitida para el UE. (NSSAI es la abreviatura de información de asistencia de selección de segmento de red, es decir, información de asistencia de selección de segmento de
15 red/información de asistencia de selección de segmento de red. Un segmento de red se identifica de manera única por un S-NSSAI individual, y un conjunto de una o más piezas de S-NSSAI se conoce como NSSAI).

En un sistema de comunicación de 5G, el elemento de red de selección de segmento de red puede ser un elemento de red de función de selección de segmento de red (network slice selection function, NSSF). En un sistema de comunicación futuro, el elemento de red de
20 selección de segmento de red puede seguir siendo un elemento de red de NSSF, o puede tener otro nombre. Esto no se limita en esta solicitud.

12. Un elemento de red de control de política es un marco de política unificado utilizado para guiar un comportamiento de red, proporciona información de política de configuración
25 para el UE, y proporciona información de regla de política, y similares para un elemento de red de función de plano de control (por ejemplo, un elemento de red de AMF o SMF).

En un sistema de comunicación de 5G, el elemento de red de control de política puede ser un elemento de red de función de control de política (policy control function, PCF). En un sistema de comunicación futuro, el elemento de red de control de política puede seguir siendo
30 un elemento de red de PCF, o puede tener otro nombre. Esto no se limita en esta solicitud.

13. Una red de datos es una red utilizada para transmitir datos.

En un sistema de comunicación de 5G, la red de datos puede ser una red de datos (data network, DN). En un sistema de comunicación futuro, la red de datos puede seguir siendo un DN, o puede tener otro nombre. Esto no se limita en esta solicitud.

- 5 14. Un elemento de red de autenticación y autorización específico de segmento de red se configura para realizar autenticación y autorización en un segmento de red específico.

10 En un sistema de comunicación de 5G, el elemento de red de autenticación y autorización específica de segmento de red puede ser un elemento de red de función de autenticación y autorización específica de segmento de red (network slice-specific authentication and authorization function, NSSAAF). En un sistema de comunicación futuro, el elemento de red de autenticación y autorización específico de segmento de red puede seguir siendo un elemento de red de NSSAAF, o puede tener otro nombre. Esto no se limita en esta solicitud.

- 15 15. Un programa sustituto de comunicación de servicio (service communication proxy, SCP) se configura para implementar una función de programa sustituto de comunicación entre funciones de red (network functions, NF). Las NF no necesitan comunicarse directamente entre sí; en su lugar, se comunican indirectamente entre sí a través del SCP. El SCP puede simplificar la red de encaminamiento de señalización.

En un sistema de comunicación futuro, el programa sustituto de comunicación de servicio puede tener alternativamente otro nombre. Esto no se limita en esta solicitud.

- 20 16. Un elemento de red de función de anclaje de seguridad (security anchor function, SEAF) se configura para retener una clave raíz (conocida como una clave de anclaje) para acceder a una red. Usualmente, un elemento de red de AMF y el elemento de red de SEAF se despliegan conjuntamente. La SEAF es una función proporcionada por la AMF, y con base en la información recibida del UE y una AUSF, es responsable de procesar la autenticación en una red (es decir, una red de acceso) que proporciona un servicio.

30 Se debe observar que el "elemento de red" se puede implementar por software. Opcionalmente, el "elemento de red" también se puede conocer como un módulo, o similar. Esto no se limita particularmente en esta solicitud. Además, en esta solicitud, para facilitar la comprensión y descripción, la descripción de "elemento de red" se omite en las descripciones parciales. Por ejemplo, el elemento de red de AMF se conoce como AMF. En este caso, la "AMF" se entiende como el elemento de red de AMF o un módulo de AMF. Las descripciones

de una situación igual o similar se omiten a continuación.

La arquitectura de red puede incluir además un elemento de red de función de repositorio de red (Network Repository Function, NRF), configurado para administrar todos los elementos de red de NF que admiten una interfaz basada en servicios. Estos elementos de red de NF se necesitan registrar primero en la NRF. Cuando las NF se buscan entre sí, las NF se encuentran al consultar la NRF.

La arquitectura de red puede incluir además un elemento de red de administración y mantenimiento de operación (operation administration and maintenance, OAM). El elemento de red de OAM clasifica el trabajo de gestión de red en tres categorías: operación (operation), administración (administration) y mantenimiento (maintenance) de acuerdo con un requisito real de operación de red de un operador. La operación es principalmente para completar el trabajo diario, tal como el análisis, la predicción, la planificación, y la configuración realizada en una red y un servicio, y el mantenimiento es principalmente una actividad de operación diaria, tal como las pruebas y la gestión de fallas realizadas en la red y el servicio.

Por ejemplo, en esta modalidad de esta solicitud, el elemento de red NRF y/o el elemento de red de OAM pueden tener además una función de certificación remota, para proporcionar un servicio de certificación de confianza. Por ejemplo, el elemento de red de NRF se utiliza como un ejemplo. El dispositivo de red de acceso tiene una capacidad de certificación de confianza o una capacidad de verificación de información de certificación. En este caso, el elemento de red de NRF puede enviar una solicitud de certificación al dispositivo de red de acceso, la NRF recibe información de certificación retornada por el dispositivo de red de acceso en respuesta a la solicitud de certificación, el elemento de red de NRF determina un resultado de certificación de confianza del dispositivo de red de acceso con base en la información de certificación y la información esperada, y el elemento de red de NRF proporciona al dispositivo de red de acceso un resultado de certificación de confianza que indica que el dispositivo de red de acceso es confiable o el dispositivo de red de acceso no es confiable.

Por ejemplo, en esta solicitud, la arquitectura de red puede incluir además un elemento de red de función de certificación remota (remote attestation function, RAF), que se conoce brevemente como un elemento de red de certificación. El elemento de red de certificación se configura para proporcionar un servicio de certificación de confianza. Por ejemplo, si el UE tiene la capacidad de certificación de confianza o la capacidad de verificación de información de certificación, el UE puede solicitar al elemento de red de certificación que realice la

certificación de confianza, y el elemento de red de certificación proporciona al UE con un resultado de certificación de confianza que indica que el UE es confiable o el UE no es confiable.

5 Por ejemplo, en esta solicitud, la arquitectura de red puede incluir además un elemento de red de función de gestión de datos de valor de confiabilidad (trustworthiness profile management function, TPMF), configurado para proporcionar al elemento de red de función de certificación remota datos de valor de confianza relacionados con una entidad certificada, es decir, un vector de confianza. Los datos de valor de confianza incluyen al menos uno de los siguientes: un número aleatorio, una clave utilizada para la certificación de confianza o
10 información de certificación esperada de la entidad certificada.

Por ejemplo, la figura 2B es un diagrama de otra arquitectura de red de acuerdo con una modalidad de esta solicitud. En esta solicitud, la arquitectura de red puede incluir además una entidad de provisión de valor de referencia (proveedores de valor de referencia), configurada para proporcionar información de certificación esperada a un elemento de red de
15 TPMF. La información de certificación esperada es un valor de referencia de información de certificación local de una entidad que tiene un requisito de certificación de confianza, es decir, una entidad certificada (por ejemplo, UE, una NF, o una red de acceso de radio).

Además, una entidad de función de red 1 y una entidad de función de red 2 en la figura 2B son elementos de red de núcleo mostrados en la figura 2A.

20 Por ejemplo, en una red 5G, un elemento de red de certificación o el elemento de red de TPMF puede ser uno de los elementos de red en una red de núcleo 5G (5G core, 5GC). Alternativamente, el elemento de red de certificación o el elemento de red de TPMF pueden ser un elemento de red de núcleo. Alternativamente, el elemento de red de certificación y el elemento de red de TPMF se pueden desplegar independientemente, o el elemento de red de
25 certificación y el elemento de red de TPMF se despliegan conjuntamente. Como se muestra en la figura 2B, el elemento de red de certificación y el elemento de red de TPMF se despliegan conjuntamente como una entidad de servicio de certificación remota, o un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Esto no se limita particularmente en esta solicitud. Por ejemplo, en las descripciones anteriores, cuando los dos
30 elementos de red que se despliegan originalmente de manera independiente cambian a elementos de red que se despliegan conjuntamente, se puede ignorar un procedimiento de interacción entre los dos elementos de red que se despliegan originalmente de manera independiente, y una función implementada por el procedimiento de interacción entre los dos

elementos de red se implementa por los elementos de red que se despliegan conjuntamente.

En la figura 2A, N1, N2, N3, N4, N6, y similares son números de secuencia de interfaz.

Se debe entender que la arquitectura de red aplicada a las modalidades de esta solicitud es simplemente un ejemplo de una arquitectura de red descrita desde una perspectiva de una arquitectura basada en servicios, y una arquitectura de red aplicable a las modalidades de esta solicitud no se limita a la misma. Las modalidades de esta solicitud son aplicables a cualquier arquitectura de red que pueda implementar funciones de los elementos de red anteriores.

Por ejemplo, en algunas arquitecturas de red, las entidades de función de red como la AMF, la SMF, la PCF, la UPF, y el UDM se conocen como elementos de red de NF. De manera alternativa, en algunas otras arquitecturas de red, un conjunto de elementos de red tal como la AMF, la SMF, la PCF, la UPF, y el UDM se puede conocer como un elemento de red de función de plano de control (Control Plane Function, CPF).

En esta solicitud, el elemento de red de certificación propuesto puede comunicarse con otro elemento de red. Por ejemplo, el elemento de red de certificación se puede comunicar con elementos de red tal como la RAN, el elemento de red de AMF, el elemento de red de SMF, y el elemento de red de UDM.

A continuación se utilizan elementos de red en un sistema de 5G como un ejemplo para describir detalles específicos de la solución. Se puede entender que, cuando la solución se aplica a un sistema de LTE o un sistema de comunicación futuro, cada elemento de red en la solución se puede reemplazar con otro elemento de red que tenga una función correspondiente. Esto no se limita en esta solicitud.

Un lado de red determina la seguridad de un lado de UE con base en una tarjeta de SIM. La lógica de seguridad básica es que la tarjeta de SIM y el lado de red retienen conjuntamente una clave compartida, y un usuario realiza una operación en la clave compartida en un proceso de acceso a la red, para realizar la autenticación y autorización.

La figura 2C es un diagrama de un procedimiento de autenticación de acuerdo con una modalidad de esta solicitud. Un proceso de autenticación específico incluye los siguientes pasos.

(1) El UE envía una solicitud de registro a una AMF por el uso de un dispositivo de red

de acceso. La solicitud de registro incluye información de identificación del UE. Alternativamente, la AMF se puede desplegar conjuntamente con una SEAF. Por ejemplo, el UE incluye un equipo móvil (Mobile Equipment, ME) y una tarjeta de módulo de identidad de abonado universal (UMTS subscriber identity module, USIM). La tarjeta de USIM es un tipo de tarjeta de SIM. UMTS es la abreviatura de sistema universal de telecomunicaciones móviles (Universal Mobile Telecommunications System).

La tarjeta de SIM en esta modalidad de esta solicitud incluye una tarjeta de SIM para la cual sólo una red realiza autenticación de identidad en la tarjeta de SIM, una tarjeta de USIM que usa un mecanismo de autenticación bidireccional, una tarjeta de eSIM (SIM incrustada) o una tarjeta de SIM blanda (blanda). El mecanismo de autenticación bidireccional significa que cuando el UE accede a la red, no sólo la red realiza la autenticación de identidad en la tarjeta de USIM, sino que también la tarjeta de USIM realiza la autenticación de identidad en la red. Las dos primeras tarjetas de SIM son tarjetas físicas y se insertan en una ranura de tarjeta de una terminal cuando se usan.

La tarjeta de eSIM es una tarjeta de SIM electrónica, y se descarga e instala en la terminal a través de una red. Diferente de una tarjeta de SIM física convencional, una idea de diseño de una tarjeta de SIM removible convencional se abandona para la tarjeta de eSIM. En su lugar, la tarjeta de SIM se incrusta directamente en un dispositivo como una parte, tal que la tarjeta de eSIM pueda reemplazar a la tarjeta de SIM física.

La tarjeta de SIM de software simplemente simula la tarjeta de SIM por el uso de software, en lugar de utilizar una tarjeta de SIM física real. Después de que el software modifica una banda base, la banda base se redirige para interactuar directamente con una capa de sistema operativo.

Los procesos de autenticación de los tipos anteriores de tarjetas de SIM son los mismos. En esta modalidad de esta solicitud, la tarjeta de USIM se usa como un ejemplo para la descripción.

(2) La AMF inicia una solicitud de autenticación a una AUSF con base en la solicitud de registro. La solicitud de autenticación incluye la información de identificación del UE.

(3) La AUSF determina un UDM que procesa una solicitud de autenticación del UE, obtiene datos de autenticación del UE, es decir, un vector de autenticación (authentication vector, AV) del UDM, y envía el AV a la AMF. El AV es un grupo de parámetros utilizado para

la autenticación, y el grupo de parámetros incluye cuatro parámetros:

RAND (RandomChallenge, número aleatorio): RAND es un número aleatorio impredecible proporcionado por la red al UE.

5 AUTN (AuthenticationToken, token de autenticación): Una función de la AUTN es proporcionar información al UE, tal que el UE pueda usar la información para autenticar la red.

10 XRES (ExpectedResponse, respuesta esperada): "X" en XRES es Esperado, indicando "esperado". XRES es un parámetro de respuesta de autenticación de UE esperado, y también se puede entender como un valor de autenticación esperado RES'. RES' se compara con RES (o RES+RES_ext) generado por el UE, para determinar si la autenticación tiene éxito.

15 KASME: KASME es una clave raíz derivada con base en CK/IK y una ID de red móvil terrestre pública (Public Land Mobile Network ID, PLMNID) de una entidad de gestión de seguridad de acceso (Access Security Management entity, ASME). Una clave de cifrado CK y una clave de protección de integridad IK se derivan con base en una clave raíz de autenticación K.

20 Específicamente, después de determinar un UDM, la AUSF envía una solicitud de vector de autenticación al UDM. La solicitud de vector de autenticación incluye la información de identificación del UE. El UDM obtiene el vector de autenticación del UE con base en la información de identificación del UE, y el UDM envía el vector de autenticación a la AUSF. La AUSF retorna el vector de autenticación a la AMF en una respuesta de autenticación.

(4) La AMF envía el vector de autenticación al dispositivo de red de acceso, y el dispositivo de red de acceso transmite de manera transparente el vector de autenticación al UE.

25 (5) Después de recibir el vector de autenticación, la tarjeta de SIM verifica la validez de un mensaje de autenticación de red central con base en un parámetro en el vector de autenticación, calcula un valor de autenticación RES, y envía RES al ME.

30 (6) El ME retorna RES a la AMF por el uso del dispositivo de red de acceso, y la AMF transfiere RES a la AUSF. Si se utiliza AKA de 5G, la AMF necesita además verificar RES, obtener un resultado de verificación del UE desde una perspectiva de una red de servicio, y enviar el resultado de verificación a la AUSF.

(7) La AUSF verifica RES, y obtiene un resultado de autenticación del UE desde una perspectiva de una red doméstica. Específicamente, RES se compara con RES', y la autenticación tiene éxito si RES y RES' son las mismas; o la autenticación falla si RES y RES' son diferentes.

- 5 (8) La AUSF retorna el resultado de autenticación del UE a la AMF. La AMF envía el resultado de autenticación del UE al dispositivo de red de acceso, y el dispositivo de red de acceso transmite de manera transparente el resultado de autenticación al UE.

Después de que el lado de red y el lado de UE completen la autenticación bidireccional, la derivación de clave se realiza con base en una clave.

- 10 Se puede enterar a partir del proceso de autenticación anterior de que la verificación de seguridad de extremo a extremo entre el lado de red y el lado de UE es una verificación desde un extremo de red hasta un extremo de tarjeta de SIM, pero no se determina la confiabilidad de un dispositivo de hardware del UE.

- 15 Por lo tanto, una modalidad de esta solicitud proporciona un método de certificación de confianza, para realizar una certificación de confianza en una terminal.

La figura 3 es un diagrama de flujo de un método de certificación de acuerdo con una modalidad de esta solicitud. En esta modalidad, el método de certificación incluye los siguientes pasos.

301: Una terminal determina la primera información de certificación.

- 20 302: La terminal envía la primera información de certificación a un primer elemento de red.

Por consiguiente, el primer elemento de red recibe la primera información de certificación de la terminal.

- 25 303: El primer elemento de red obtiene un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación y la primera información esperada.

Específicamente, el primer resultado de certificación de confianza indica que la terminal es confiable o no confiable.

En esta modalidad, el primer elemento de red puede determinar el primer resultado de certificación de confianza de la terminal con base en la primera información de certificación de la terminal y la primera información esperada, para implementar la certificación de confianza de la terminal, es decir, determinar si la terminal es confiable.

- 5 En una posible modalidad, como se muestra en la figura 3, el método de certificación incluye además:

304: El primer elemento de red envía el primer resultado de certificación de confianza a la terminal.

- 10 Se puede enterar de que, en esta modalidad, el primer elemento de red retroalimenta un resultado de certificación de confianza de la terminal a la terminal, tal que la terminal obtenga el resultado de certificación de confianza de la terminal.

- 15 En una posible modalidad, la primera información de certificación en el paso 301 incluye un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación local al usar una clave simétrica, y la clave simétrica es una clave usada para certificación de confianza. La clave simétrica significa que la terminal y el primer elemento de red tienen una misma clave utilizada para la certificación de confianza. El primer elemento de red o un tercer elemento de red genera un primer número aleatorio para cada vez de certificación de confianza de la terminal, y proporciona el primer número aleatorio a la terminal. Para una manera en la que la terminal obtiene el primer número aleatorio, hacer referencia a las descripciones relacionadas del paso 20 C403, el paso C404, y el paso C405. Los detalles no se describen de nuevo en la presente.

- 25 La información de certificación local es información que se necesita certificar en la terminal. Por ejemplo, la información de certificación local incluye una cuota (quota) y/o un registro de certificación (registro de eventos). El registro de certificación es información de proceso de certificación de una plataforma informática de confianza soportada por la terminal. La cuota incluye un resumen del registro de certificación, y el resumen del registro de certificación se obtiene al realizar el cálculo de hash en el registro de certificación.

- 30 La primera información esperada incluye un primer valor de verificación esperado, y el primer valor de verificación esperado se obtiene al procesar el primer número aleatorio y la primera información de certificación esperada al usar la clave simétrica. El primer elemento de red genera un primer número aleatorio por cada vez de certificación de confianza de la

terminal, o el tercer elemento de red genera un primer número aleatorio por cada vez de certificación de confianza de la terminal, y proporciona el primer número aleatorio al primer elemento de red. La primera información de certificación esperada es un valor de referencia de la información de certificación local de la terminal. El primer elemento de red obtiene la
5 primera información de certificación esperada correspondiente con base en la información de identificación de la terminal. Para un proceso específico, hacer referencia a las descripciones relacionadas del paso C403, el paso C404, y el paso C405. En el paso 303, el primer elemento de red se entera, a través de la comparación, de si el primer valor de verificación esperado es el mismo que el primer valor de verificación, y cuando se entera, a través de la comparación,
10 de que el primer valor de verificación esperado es el mismo que el primer valor de verificación, el primer resultado de certificación de confianza de la terminal es que la terminal es confiable; o cuando se entera, a través de la comparación, de que el primer valor de verificación esperado es diferente del primer valor de verificación, el primer resultado de certificación de confianza de la terminal es que la terminal no es confiable.

15 En una posible modalidad, la primera información de certificación en el paso 301 incluye además la información de certificación local de la terminal. La primera información esperada incluye además la primera información de certificación esperada. Por ejemplo, en el paso 303, el primer elemento de red se entera, a través de la comparación, de si la primera información de certificación esperada es la misma que la información de certificación local, y
20 se entera, a través de la comparación, de si el primer valor de verificación esperado es el mismo que el primer valor de verificación. Cuando se entera, a través de la comparación, de que la primera información de certificación esperada es la misma que la información de certificación local, y el primer valor de verificación esperado es el mismo que el primer valor de verificación, el primer resultado de certificación de confianza de la terminal es que la
25 terminal es confiable; o cuando se entera, a través de la comparación, de que la primera información de certificación esperada es diferente de la información de certificación local, y/o el primer valor de verificación esperado es diferente del primer valor de verificación, el primer resultado de certificación de confianza de la terminal es que la terminal no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros,
30 es decir, el primer valor de verificación y el primer valor de verificación esperado, y la información de certificación local y la primera información de certificación esperada son las mismas, para garantizar una mayor fiabilidad de un resultado de certificación de confianza de la terminal.

Por ejemplo, la primera información de certificación puede incluir además el primer

número aleatorio, para indicar que el primer valor de verificación corresponde al primer número aleatorio. En otras palabras, el primer valor de verificación se genera con base en el primer número aleatorio. De manera similar, la primera información esperada puede incluir además el primer número aleatorio, para indicar que el primer valor de verificación esperado
5 corresponde al primer número aleatorio. En otras palabras, el primer valor de verificación esperado se genera con base en el primer número aleatorio. En el paso 303, el primer elemento de red se entera además, a través de la comparación, de si el primer número aleatorio en la primera información de certificación es el mismo que el primer número aleatorio en la primera información esperada. Cuando se entera, a través de la comparación, de que la
10 primera información de certificación esperada es la misma que la información de certificación local, el primer valor de verificación esperado es el mismo que el primer valor de verificación, y el primer número aleatorio en la primera información de certificación es el mismo que el primer número aleatorio en la primera información esperada, el primer resultado de certificación de confianza de la terminal es que la terminal es confiable; o cuando se entera,
15 a través de la comparación, de que la primera información de certificación esperada es diferente de la información de certificación local, y/o el primer valor de verificación esperado es diferente del primer valor de verificación, y/o el primer número aleatorio en la primera información de certificación es diferente del primer número aleatorio en la primera información esperada, el primer resultado de certificación de confianza de la terminal es que la terminal
20 no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los tres grupos de parámetros, es decir, el primer valor de verificación y el primer valor de verificación esperado, la información de certificación local y la primera información de certificación esperada, y el primer número aleatorio en la primera información de certificación y el primer número aleatorio en la primera información esperada son los mismos, para mejorar aún más
25 la fiabilidad del resultado de certificación de confianza de la terminal.

En una posible modalidad, la primera información de certificación puede incluir además un número de secuencia que corresponde a la primera información de certificación, y el número de secuencia identifica la primera información de certificación. Por ejemplo, el número de secuencia se puede ajustar alternativamente a un mismo nivel que la primera información
30 de certificación. Por ejemplo, la terminal envía un mensaje de respuesta de certificación al primer elemento de red. El mensaje de respuesta de certificación incluye la primera información de certificación y el número de secuencia.

En una posible modalidad, la clave simétrica es cualquiera de las siguientes:

Clave raíz utilizada para la certificación de confianza: Para ser específicos, la terminal se preconfigura con una clave raíz especialmente utilizada para la certificación de confianza, y comparte de forma segura la clave raíz con un lado de red (por ejemplo, el primer elemento de red), tal que el primer elemento de red y la terminal realicen la certificación de confianza con base en la clave raíz.

Primera clave derivada: La primera clave derivada se deriva de la clave raíz utilizada para la certificación de confianza. Para ser específicos, la terminal se preconfigura con una clave raíz especialmente utilizada para la certificación de confianza, y comparte de manera segura la clave raíz con el lado de red. La terminal y el lado de red derivan la primera clave derivada con base en un mismo algoritmo de derivación, tal que el primer elemento de red y la terminal realicen la certificación de confianza con base en la primera clave derivada.

Segunda clave derivada: La segunda clave derivada se deriva de una clave raíz utilizada para la autenticación. Para ser específicos, la terminal se preconfigura con la clave raíz utilizada especialmente para la autenticación, y comparte de manera segura la clave raíz con el lado de red. La terminal y el lado de red derivan la segunda clave derivada con base en un mismo algoritmo de derivación, tal que el primer elemento de red y la terminal realicen la certificación de confianza con base en la segunda clave derivada.

Tercera clave derivada: La tercera clave derivada se deriva de una clave de autenticación. La terminal y el lado de red derivan la tercera clave derivada con base en un mismo algoritmo de derivación y la clave de autenticación. El primer elemento de red y la terminal realizan la certificación de confianza con base en la tercera clave derivada.

En una posible modalidad, el método de certificación incluye además:

El primer elemento de red realiza la derivación de clave con base en la clave simétrica, para obtener una cuarta clave derivada, donde la cuarta clave derivada es cualquiera de las siguientes: una primera clave de anclaje y la clave de autenticación.

En esta modalidad, el primer elemento de red puede continuar realizando la derivación de clave con base en la clave simétrica. Por ejemplo, el primer elemento de red envía una primera clave de anclaje al segundo elemento de red. Para otro ejemplo, el primer elemento de red envía la clave de autenticación a un elemento de red de autenticación.

A continuación se describe específicamente un método de certificación en una modalidad de esta solicitud por el uso de un ejemplo en el que una clave simétrica es una

primera clave derivada.

La figura 4A es un diagrama de un procedimiento de certificación de confianza de acuerdo con una modalidad de esta solicitud. En esta modalidad, se usa un ejemplo en el que el UE es un teléfono móvil 401, y se usa un ejemplo en el que una tecnología de certificación de confianza es un TPM. El teléfono móvil 401 incluye una tarjeta de SIM. La tarjeta de SIM en esta modalidad de esta solicitud incluye una tarjeta de SIM para la cual sólo una red realiza autenticación de identidad en la tarjeta de SIM, una tarjeta de USIM, una tarjeta de eSIM o una tarjeta de SIM blanda. Una clave raíz K utilizada para la autenticación y una clave raíz K_{TPM} utilizada para la certificación de confianza se preestablecen en la tarjeta de SIM. En una etapa de producción, un fabricante de tarjeta de SIM preestablece una función de TPM en la tarjeta de SIM, y actualiza la clave raíz K_{TPM} en la tarjeta de SIM a un servidor de recursos 402 de un operador a través de un canal seguro. De esta manera, en un proceso posterior de uso del teléfono móvil 401, se puede realizar una certificación de confianza remota entre una red de operador 403 y el teléfono móvil 401 con base en la clave raíz K_{TPM} . Específicamente, la red de operador 403 realiza la derivación de clave con base en la clave raíz K_{TPM} en el servidor de recursos 402, y el teléfono móvil 401 realiza la derivación de clave con base en la clave raíz K_{TPM} en el teléfono móvil 401.

Además, la clave raíz K en la tarjeta de SIM se actualiza adicionalmente al servidor de recursos 402 del operador a través del canal seguro. De esta manera, la red de operador 403 puede realizar la autenticación en el teléfono móvil con base en la clave raíz K utilizada para la autenticación. En esta modalidad, para un proceso específico de realizar la autenticación en el teléfono móvil, se hace referencia a las descripciones en la figura 2C. Los detalles no se describen de nuevo en la presente.

La figura 4B es un diagrama de una arquitectura de clave de acuerdo con una modalidad de esta solicitud. Tanto un lado de red como un lado de UE realizan la derivación de clave con base en la arquitectura de clave en la figura 4B. Una red móvil terrestre pública local es una red móvil terrestre pública local, que es HPLMN para abreviar. Por ejemplo, en el lado de red, una clave K_{RAF} es una clave que se va a utilizar por un elemento de red de RAF, una clave K_{SEAF} es una clave que se va a utilizar por un elemento de red de SEAF, la clave K_{SEAF} es una clave de anclaje, una clave $K_{\text{AMF-RA}}$ es una clave que se va a utilizar por un elemento de red de AMF, y una clave $K_{\text{gNB-RA}}$ es una clave que se va a utilizar por un dispositivo de red de acceso.

A continuación se describe un proceso de certificación de confianza de UE en la figura

4A.

La figura 4C es un diagrama de flujo de interacción de un método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

- 5 C401: El UE envía una solicitud de registro a un segundo elemento de red, donde la solicitud de registro incluye información de identificación del UE.

Específicamente, en esta modalidad, el segundo elemento de red puede ser una AMF, o el segundo elemento de red es un elemento de red en el que la AMF y una SEAF se despliegan conjuntamente. Por ejemplo, la solicitud de registro incluye además una tecnología de certificación de confianza (es decir, un tipo de certificación de confianza, es decir, el tipo anterior de informática de confianza) soportada por el UE. Para otro ejemplo, la solicitud de registro incluye además una versión de sistema operativo y/o una versión de aplicación (application, APP) del UE. Por ejemplo, un elemento de red de TPMF puede obtener un valor de referencia de la información de certificación local del UE, es decir, la primera información de certificación esperada, con base en la información de identificación del UE y la versión de sistema operativo y/o la versión de aplicación del UE. Por ejemplo, como se muestra en las figuras 2B, el elemento de red de TPMF obtiene la primera información de certificación esperada del UE a partir de una entidad de provisión de valor de referencia con base en la información de identificación del UE y la versión de sistema operativo y/o la versión de aplicación del UE.

Además, el UE puede enviar la solicitud de registro al segundo elemento de red por el uso de un dispositivo de red de acceso.

La información de identificación del UE incluye cualquiera de los siguientes: información de identificador permanente de suscripción (subscription permanent identifier, SUPI), información de identificador oculto de suscripción (subscription concealed identifier, SUCI), información de identidad de suscriptor móvil internacional (international mobile subscriber identity, IMSI), información de identificador de equipo permanente (permanent equipment identifier, PEI), información de identidad de equipo móvil internacional (international mobile equipment identity, IMEI), información de identificador de suscripción público genérico (generic public subscription identifier, GPSI), e información de número de ISDN internacional de suscriptor móvil (mobile subscriber international ISDN number, MSISDN).

C402: El segundo elemento de red envía una primera solicitud de certificación a un primer elemento de red, donde la primera solicitud de certificación incluye la información de identificación del UE.

5 Por consiguiente, el primer elemento de red recibe la primera solicitud de certificación del segundo elemento de red.

Específicamente, la primera solicitud de certificación se utiliza para activar el primer elemento de red para realizar la certificación de confianza en el UE. En esta modalidad, el primer elemento de red puede ser un elemento de red de RAF. El primer elemento de red obtiene un primer vector de confianza con base en la información de identificación del UE.
10 Para una manera en la que el primer elemento de red obtiene el primer vector de confianza, hacer referencia al paso C403, el paso C404, y el paso C405.

C403: El primer elemento de red envía una solicitud de vector de confianza a un tercer elemento de red, donde la solicitud incluye la información de identificación del UE.

15 Específicamente, en esta modalidad, el tercer elemento de red puede ser un elemento de red de TPMF. Opcionalmente, un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Opcionalmente, el elemento de red de TPMF y el elemento de red de RAF se despliegan conjuntamente.

C404: El tercer elemento de red genera el primer vector de confianza.

20 Específicamente, si la información de identificación del UE es un SUCI, el tercer elemento de red descifra el SUCI para obtener un SUPI, y obtiene, a través de una consulta basada en el SUPI, la primera evidencia de información de certificación esperada y una clave simétrica K_{RAF} que corresponden al UE. La clave simétrica K_{RAF} se deriva del tercer elemento de red con base en una clave raíz K_{TPM} . El tercer elemento de red procesa la primera evidencia de información de certificación esperada' y un primer número aleatorio nonce por el uso de la
25 clave simétrica K_{RAF} , para generar un primer valor de verificación esperado HMAC'. Por ejemplo, el primer vector de confianza incluye la primera información esperada, y la primera información esperada incluye el primer valor de verificación esperado HMAC'. Para otro ejemplo, la primera información esperada incluye además la primera evidencia de información de certificación esperada'. Opcionalmente, la primera información esperada incluye además
30 el primer número aleatorio nonce. Por ejemplo, la primera información esperada Xatt' es un valor de combinación del primer número aleatorio nonce, la primera evidencia de información

de certificación esperada', y el primer valor de verificación esperado HMAC', y Xatt' se puede obtener a través del empalme en una secuencia del primer número aleatorio nonce, la primera evidencia de información de certificación esperada', y el primer valor de verificación esperado HMAC'. Por ejemplo, el primer vector de confianza incluye además la clave simétrica K_{RAF} .

- 5 Si la información de identificación del UE no es un SUCI, el tercer elemento de red procesa la información de identificación del UE con base en un procedimiento de procesamiento del SUPI, y también genera el primer vector de confianza.

El primer número aleatorio nonce puede ser un número aleatorio que se genera por el tercer elemento de red y que corresponde a la información de identificación del UE. En otras palabras, el tercer elemento de red genera un primer número aleatorio para cada vez de certificación de confianza del UE. El tercer elemento de red puede enviar el primer número aleatorio al UE por el uso del primer elemento de red, es decir, de una manera de unidifusión. Específicamente, el tercer elemento de red puede usar el primer vector de confianza para transportar el primer número aleatorio, y cuando se envía una segunda solicitud de certificación al UE, el primer elemento de red usa la segunda solicitud de certificación para portar el primer número aleatorio. Para otro ejemplo, el tercer elemento de red puede transmitir alternativamente el primer número aleatorio nonce a una pluralidad de UE. La pluralidad de UE son dos o más UE, y la pluralidad de UE incluye el UE en esta modalidad.

Por ejemplo, el primer valor de verificación esperado HMAC' se genera al procesar la primera evidencia de información de certificación esperada' y el primer número aleatorio nonce al usar un algoritmo de HMAC y la clave simétrica K_{RAF} . El algoritmo de HMAC es un método para construir un código de autenticación de mensaje por el uso de una función de hash unidireccional. H en HMAC significa hash. La función de hash unidireccional utilizada en HMAC no se limita a un tipo. Cualquier función de hash unidireccional de alta resistencia se puede utilizar en HMAC. Si se diseña una nueva función de hash unidireccional en el futuro, también se puede utilizar la nueva función de hash unidireccional. La función de hash unidireccional puede ser MD5 (Algoritmo de resumen de mensaje 5), SHA (Algoritmo de hash seguro)-1, SHA-256, o SHA-384. MD5 se utiliza para realizar una operación criptográfica en bloques de datos con diferentes longitudes, para obtener un valor de 128 bits. SHA-1 puede realizar una operación en datos de cualquier longitud, para generar un valor de 160 bits.

C405: El tercer elemento de red envía el primer vector de confianza al primer elemento de red.

Otra manera en la que el primer elemento de red obtiene el primer vector de confianza es: El primer elemento de red realiza el paso C403, el paso C404, y el paso C405. Una diferencia es que en el paso C404, el primer vector de confianza generado por el tercer elemento de red incluye la clave simétrica K_{RAF} , el primer número aleatorio nonce y la primera evidencia de información de certificación esperada'. De esta manera, el primer elemento de red procesa la primera evidencia de información de certificación esperada' y el primer número aleatorio nonce por el uso de la clave simétrica K_{RAF} , para generar el primer valor de verificación esperado HMAC'. Alternativamente, el primer vector de confianza generado por el tercer elemento de red incluye la clave simétrica K_{RAF} y la primera evidencia de información de certificación esperada', y el primer elemento de red procesa la primera evidencia de información de certificación esperada' y el primer número aleatorio nonce por el uso de la clave simétrica K_{RAF} , para generar el primer valor de verificación esperado HMAC'. En este caso, el primer número aleatorio nonce utilizado por el primer elemento de red puede ser un número aleatorio que se genera por el primer elemento de red y que corresponde a la información de identificación del UE. En otras palabras, el primer elemento de red genera un primer número aleatorio para cada vez de certificación de confianza del UE. De manera similar, el primer elemento de red puede enviar el primer número aleatorio al UE de una manera de unidifusión o difusión. Cuando se usa la manera de unidifusión, cuando se envía la segunda solicitud de certificación al UE, el primer elemento de red puede usar la segunda solicitud de certificación para llevar el primer número aleatorio. Cuando se usa la manera de transmisión, el tercer elemento de red puede transmitir el primer número aleatorio nonce a una pluralidad de UE. La pluralidad de UE son dos o más UE, y la pluralidad de UE incluye el UE en esta modalidad.

En este caso, de manera similar, la primera información esperada incluye el primer valor de verificación esperado HMAC'. Por ejemplo, la primera información esperada incluye además la primera evidencia de información de certificación esperada'. Opcionalmente, la primera información esperada incluye además el primer número aleatorio nonce.

C406: El primer elemento de red envía la segunda solicitud de certificación al UE.

La segunda solicitud de certificación se utiliza para activar el UE para generar la primera información de certificación. Opcionalmente, cuando el primer elemento de red o el tercer elemento de red proporciona el primer número aleatorio al UE de la manera de unidifusión, la segunda solicitud de certificación incluye el primer número aleatorio. En la modalidad mostrada en las FIGURAS 4C, el primer elemento de red envía la segunda solicitud

de certificación al UE por el uso del segundo elemento de red. Específicamente, el primer elemento de red envía una primera respuesta de certificación al segundo elemento de red. La primera respuesta de certificación porta el primer número aleatorio nonce. El segundo elemento de red envía la segunda solicitud de certificación al UE. La solicitud porta el primer
5 número aleatorio nonce. Específicamente, la primera respuesta de certificación enviada por el primer elemento de red activa el segundo elemento de red para enviar la segunda solicitud de certificación al UE.

Cuando el primer elemento de red o el tercer elemento de red proporciona el primer número aleatorio al UE de la manera de transmisión, la segunda solicitud de certificación no
10 necesita portar el primer número aleatorio, y la segunda solicitud de certificación sólo necesita activar el UE para generar la primera información de certificación. En este caso, el primer elemento de red envía la segunda solicitud de certificación al UE por el uso del segundo elemento de red.

C407: El UE determina la primera información de certificación.

15 Específicamente, en esta modalidad, el UE procesa el primer número aleatorio nonce y la evidencia de información de certificación local por el uso de la clave simétrica K_{RAF} , para generar el primer valor de verificación HMAC. La primera información de certificación incluye un primer valor de verificación HMAC. Por ejemplo, la primera información de certificación incluye además la evidencia de información de certificación local. Por ejemplo, la primera
20 información de certificación Xatt es un valor de combinación de la evidencia de información de certificación local y el primer valor de verificación HMAC, y Xatt se puede obtener a través del empalme en una secuencia de la evidencia de información de certificación local y el primer valor de verificación HMAC. Opcionalmente, la primera información de certificación incluye además el primer número aleatorio nonce. Por ejemplo, la primera información de certificación
25 Xatt es un valor de combinación del primer número aleatorio nonce, la evidencia de información de certificación local y el primer valor de verificación HMAC, y Xatt se puede obtener a través del empalme en una secuencia del primer número aleatorio nonce, la evidencia de información de certificación local, y el primer valor de verificación HMAC.

C408: El UE envía la primera información de certificación al primer elemento de red.

30 Por ejemplo, la primera información esperada incluye además el primer número aleatorio nonce. Cuando el primer número aleatorio nonce es un número aleatorio que se genera por el tercer elemento de red y que corresponde a la información de identificación del

UE, el UE envía una segunda respuesta de certificación al segundo elemento de red. El segundo elemento de red envía la segunda respuesta de certificación al primer elemento de red.

5 Específicamente, la segunda respuesta de certificación incluye la primera información de certificación Xatt. Opcionalmente, la segunda respuesta de certificación puede incluir además el primer número aleatorio nonce y/o la evidencia de información de certificación local.

10 Para otro ejemplo, cuando el primer número aleatorio nonce es un número aleatorio común que se transmite por el primer elemento de red a una pluralidad de UE por adelantado, el UE envía la primera información de certificación Xatt al primer elemento de red por el uso del segundo elemento de red. Opcionalmente, cuando se envía la primera información de certificación Xatt, el UE porta además el primer número aleatorio nonce y/o la evidencia de información de certificación local.

15 C409: El primer elemento de red compara Xatt y Xatt', y genera un primer resultado de certificación de confianza. Si Xatt y Xatt' son consistentes, el resultado de la certificación es que el UE es confiable; o si Xatt y Xatt' son inconsistentes, el resultado de certificación es que el UE no es confiable.

20 Por ejemplo, la primera información de certificación Xatt es el valor de combinación del primer número aleatorio nonce, la evidencia de información de certificación local, y el primer valor de verificación HMAC. Cuando se compara Xatt y Xatt', el primer elemento de red puede extraer por separado el primer número aleatorio nonce, la evidencia de información de certificación local y el primer valor de verificación HMAC en Xatt, y el primer número aleatorio nonce, la primera evidencia de información de certificación esperada', y el primer valor de verificación esperado HMAC' en Xatt'; enterarse, a través de la comparación, de si el primer número aleatorio nonce en Xatt es el mismo que el primer número aleatorio nonce en Xatt';
25 enterarse, a través de la comparación, de si la evidencia de información de certificación local es la misma que la primera evidencia de información de certificación esperada'; y enterarse, a través de la comparación, de si el primer valor de verificación HMAC es el mismo que el primer valor de verificación esperado HMAC'. Cuando los resultados de comparación de los tres artículos son todos "iguales", indica que Xatt y Xatt' son consistentes; o cuando los
30 resultados de comparación de los tres artículos no son todos "iguales", Xatt y Xatt' son inconsistentes.

Para otro ejemplo, cuando el primer vector de confianza incluye además la clave

simétrica K_{RAF} , la clave simétrica K_{RAF} se puede usar para procesar el primer número aleatorio nonce y la primera evidencia de información de certificación esperada' para generar un valor de verificación, y el primer valor de verificación HMAC se verifica con base en el valor de verificación generado.

- 5 C410: El primer elemento de red retorna el primer resultado de certificación de confianza al segundo elemento de red, y entonces el segundo elemento de red retorna el primer resultado de certificación de confianza al UE.

10 Cuando el resultado de certificación indica que el UE es confiable, un lado del UE y un lado de la red pueden continuar realizando la derivación de clave con base en la clave simétrica K_{RAF} . Como se muestra en la figura 4B, una clave de anclaje $K_{SEAF-RA}$ puede continuar derivándose de la clave simétrica K_{RAF} , una clave K_{AMF-RA} que se va a utilizar por la AMF puede continuar derivándose de la clave de anclaje $K_{SEAF-RA}$, y una clave K_{gNB-RA} que se va a utilizar por el dispositivo de red de acceso (es decir, una gNB) puede continuar derivándose de la clave K_{AMF-RA} .

15 Por ejemplo, cuando el primer número aleatorio nonce es un número aleatorio común que se transmite por el primer elemento de red a una pluralidad de UE por adelantado, el UE puede informar directamente la primera información de certificación al primer elemento de red, y el primer elemento de red no necesita enviar la segunda solicitud de certificación al UE. Por ejemplo, el UE puede reportar periódicamente la primera información de certificación al primer elemento de red, o el UE reporta la primera información de certificación al primer elemento de red con base en otra política. La otra política es, por ejemplo, informar la primera información de certificación al primer elemento de red cada vez que el UE se enciende o después de que el UE solicite un servicio. Para otro ejemplo, cuando el UE reporta directamente la primera información de certificación al primer elemento de red, el primer elemento de red puede realizar una certificación de confianza con base en la primera información de certificación y la primera información esperada. De manera alternativa, antes de que el primer elemento de red realice la certificación de confianza con base en la primera información de certificación y la primera información esperada, si el primer elemento de red recibe la primera solicitud de certificación del segundo elemento de red, donde la primera solicitud de certificación incluye la información de identificación del UE, la primera solicitud de certificación se utiliza para activar el primer elemento de red para iniciar la certificación de confianza del UE. En otras palabras, el primer elemento de red realiza la certificación de confianza con base en la primera información de certificación y la primera información esperada sólo después de recibir la

20

25

30

primera solicitud de certificación.

A continuación se describe específicamente un método de certificación en una modalidad de esta solicitud por el uso de un ejemplo en el que una clave simétrica es una segunda clave derivada.

5 Diferente de la figura 4A, en esta modalidad, un chip de SIM en el UE no se preconfigura con una clave raíz K_{TPM} utilizada para la certificación de confianza. Sin embargo, una tarjeta de SIM aún se preconfigura con una clave raíz K utilizada para la autenticación. Además, la clave raíz en la tarjeta de SIM se actualiza adicionalmente a un servidor de recursos de un operador a través de un canal seguro. De esta manera, una red de operador
10 puede realizar la autenticación en un teléfono móvil con base en la clave raíz K utilizada para la autenticación. En esta modalidad, una clave de autenticación K_{AUSF} que se va a utilizar por un elemento de red de autenticación y una clave simétrica K_{RAF} que se va a utilizar por un primer elemento de red se derivan con base en la clave raíz K .

15 La figura 4D es un diagrama de otra arquitectura de clave de acuerdo con una modalidad de esta solicitud. Tanto un lado de red como un lado de UE realizan la derivación de clave con base en la arquitectura de clave en la figura 4D.

A continuación se describe un proceso de certificación de confianza de UE.

20 La figura 4E es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

E401: El UE envía una solicitud de registro a un segundo elemento de red, donde la solicitud incluye información de identificación del UE.

25 Específicamente, la negociación de capacidad de confianza se realiza entre el UE y una red. En esta modalidad, el segundo elemento de red puede ser un elemento de red de AMF, o el segundo elemento de red es un elemento de red en el que la AMF y una SEAF se despliegan conjuntamente. Para obtener descripciones específicas del paso E401, hacer referencia a las descripciones relacionadas del paso C401. Los detalles no se describen de nuevo en la presente.

30 E402: El segundo elemento de red envía una primera solicitud de certificación a un primer elemento de red, donde la solicitud incluye la información de identificación del UE.

5 Específicamente, el primer elemento de red obtiene un primer vector de confianza correspondiente con base en la información de identificación del UE. Para un proceso específico en el que el primer elemento de red obtiene el primer vector de confianza correspondiente con base en la información de identificación del UE, hacer referencia a las descripciones relacionadas que corresponden a la figura 4C. Se incluyen al menos dos métodos de obtención. Además, el segundo elemento de red envía una solicitud de autenticación a un elemento de red de autenticación, y el elemento de red de autenticación envía una solicitud de vector de autenticación a un tercer elemento de red. Una secuencia de envío de la primera solicitud de certificación y la solicitud de autenticación no se limita en particular.

En esta modalidad, para un proceso específico de realizar la autenticación en el UE, se hace referencia a las descripciones en la figura 2C. Los detalles no se describen de nuevo en la presente.

15 En esta modalidad, el primer elemento de red puede ser un elemento de red de RAF. El tercer elemento de red puede ser un elemento de red de TPMF. Opcionalmente, un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Opcionalmente, el elemento de red de TPMF y el elemento de red de RAF se despliegan conjuntamente.

20 E403: El primer elemento de red envía una solicitud de vector de confianza al tercer elemento de red, donde la solicitud incluye la información de identificación del UE. El elemento de red de autenticación envía la solicitud de vector de autenticación al tercer elemento de red.

De manera similar, una secuencia de envío de la solicitud de vector de confianza y la solicitud de vector de autenticación no se limita en particular.

25 E404: El tercer elemento de red genera el primer vector de confianza. El tercer elemento de red genera un vector de autenticación.

Para obtener descripciones específicas del paso E404, hacer referencia a las descripciones relacionadas del paso C404. Los detalles no se describen de nuevo en la presente. Una clave simétrica K_{RAF} se deriva por el tercer elemento de red con base en una clave raíz K utilizada para la autenticación.

30 E405: El tercer elemento de red envía el primer vector de confianza al primer elemento de red, y el tercer elemento de red envía el vector de autenticación al elemento de red de

autenticación.

E406: El primer elemento de red envía una segunda solicitud de certificación al UE, y el elemento de red de autenticación envía una solicitud de autenticación al UE.

5 Específicamente, para un proceso específico en el que el primer elemento de red envía la segunda solicitud de certificación al UE, hacer referencia a las descripciones relacionadas del paso C406. Los detalles no se describen de nuevo en la presente. La solicitud de autenticación incluye el vector de autenticación.

10 Por ejemplo, cuando el segundo elemento de red envía la segunda solicitud de certificación y la solicitud de autenticación al UE, la segunda solicitud de certificación y la solicitud de autenticación se pueden clasificar en dos solicitudes, y las dos solicitudes se envían por separado. De manera alternativa, la solicitud de autenticación se puede reutilizar, y la segunda solicitud de certificación se porta en la solicitud de autenticación. Opcionalmente, la solicitud de autenticación puede llevar información portada en la segunda solicitud de certificación, por ejemplo, un primer número aleatorio.

15 E407: El UE determina la primera información de certificación, y determina un valor de autenticación.

Para obtener descripciones específicas del paso E407, hacer referencia a las descripciones relacionadas del paso C407. Los detalles no se describen de nuevo en la presente.

20 E408: El UE envía la primera información de certificación y el valor de autenticación al primer elemento de red.

25 Para obtener descripciones específicas del envío de la primera información de certificación en el paso E408, hacer referencia a las descripciones relacionadas del paso C408. Los detalles no se describen de nuevo en la presente. Por ejemplo, cuando el UE envía el valor de autenticación al primer elemento de red, específicamente, el UE envía una respuesta de autenticación al segundo elemento de red. La respuesta de autenticación incluye el valor de autenticación. El segundo elemento de red reenvía la respuesta de autenticación al primer elemento de red.

30 E409: El primer elemento de red compara X_{att} y X_{att}' , y genera un primer resultado de certificación de confianza. El elemento de red de autenticación compara RES y RES' , y genera

un resultado de autenticación.

Específicamente, para obtener descripciones específicas de que el primer elemento de red compara X_{att} y X_{att}' , y genera el primer resultado de certificación de confianza, hacer referencia a las descripciones relacionadas del paso C409. Los detalles no se describen de nuevo en la presente.

El primer elemento de red deriva una primera clave de anclaje con base en la clave simétrica K_{RAF} , y envía la primera clave de anclaje al segundo elemento de red. El elemento de red de autenticación deriva una segunda clave de anclaje con base en una clave de autenticación K_{AUSF} , y envía la segunda clave de anclaje al segundo elemento de red. Además, el segundo elemento de red determina una tercera clave de anclaje, y la tercera clave de anclaje se utiliza como un anclaje obtenido a través de la derivación de clave posterior. Opcionalmente, el segundo elemento de red puede usar la primera clave de anclaje como la tercera clave de anclaje. Opcionalmente, el segundo elemento de red puede obtener la tercera clave de anclaje con base en la primera clave de anclaje y la segunda clave de anclaje. Por ejemplo, la tercera clave de anclaje se obtiene a través del empalme con base en la primera clave de anclaje y la segunda clave de anclaje. De manera alternativa, una parte se intercepta como la tercera clave de anclaje después de que se realiza el empalme con base en la primera clave de anclaje y la segunda clave de anclaje. Alternativamente, la tercera clave de anclaje se obtiene al realizar una operación de O exclusiva con base en la primera clave de anclaje y la segunda clave de anclaje.

A continuación se describe específicamente un método de certificación en una modalidad de esta solicitud por el uso de un ejemplo en el que una clave simétrica es una tercera clave derivada.

Diferente de la figura 4A, en esta modalidad, un chip de SIM en el UE no se preconfigura con una clave raíz K_{TPM} utilizada para la certificación de confianza. Sin embargo, una tarjeta de SIM aún se preconfigura con una clave raíz K utilizada para la autenticación. Además, la clave raíz en la tarjeta de SIM se actualiza adicionalmente a un servidor de recursos de un operador a través de un canal seguro. De esta manera, una red de operador puede realizar la autenticación en un teléfono móvil con base en la clave raíz K utilizada para la autenticación. En esta modalidad, una clave de autenticación K_{AUSF} que se va a utilizar por un elemento de red de autenticación se deriva con base en la clave raíz K , y después de que la autenticación en el UE tiene éxito, una clave simétrica K_{RAF} que se va a utilizar por un primer elemento de red se deriva con base en la clave de autenticación K_{AUSF} .

La figura 4F es un diagrama de otra arquitectura de clave de acuerdo con una modalidad de esta solicitud. Tanto un lado de red como un lado de UE realizan la derivación de clave con base en la arquitectura de clave en la figura 4F.

A continuación se describe un proceso de certificación de confianza de UE.

5 La figura 4G es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

G401: El UE envía una solicitud de registro a un segundo elemento de red, donde la solicitud incluye información de identificación del UE.

10 Específicamente, la negociación de capacidad de confianza se realiza entre el UE y una red. En esta modalidad, el segundo elemento de red puede ser un elemento de red de AMF, o el segundo elemento de red es un elemento de red en el que la AMF y una SEAF se despliegan conjuntamente. Para obtener descripciones específicas del paso G401, hacer referencia a las descripciones relacionadas del paso C401. Los detalles no se describen de
15 nuevo en la presente.

G402: El segundo elemento de red envía una primera solicitud de certificación a un primer elemento de red, donde la solicitud incluye la información de identificación del UE.

Específicamente, el segundo elemento de red envía una solicitud de autenticación a un elemento de red de autenticación, y el elemento de red de autenticación envía una solicitud
20 de vector de autenticación a un tercer elemento de red. Una secuencia de envío de la primera solicitud de certificación y la solicitud de autenticación no se limita en particular.

En esta modalidad, para un proceso específico de realizar la autenticación en el UE, se hace referencia a las descripciones en la figura 2C. Los detalles no se describen de nuevo en la presente. Hasta que el elemento de red de autenticación compare RES y RES', cuando
25 se entera, a través de la comparación, de que RES y RES' son las mismas, el elemento de red de autenticación deriva una clave simétrica K_{RAF} con base en una clave de autenticación K_{AUSF} .

El primer elemento de red obtiene un primer vector de confianza correspondiente con base en la información de identificación del UE. Para un proceso específico en el que el primer
30 elemento de red obtiene el primer vector de confianza correspondiente con base en la

información de identificación del UE, hacer referencia a las descripciones relacionadas que corresponden a la figura 4C. Se incluyen al menos dos métodos de obtención. Una diferencia es que el tercer elemento de red envía el primer vector de confianza generado al elemento de red de autenticación, y después de que la autenticación en el UE tiene éxito, el elemento de red de autenticación envía el primer vector de confianza al primer elemento de red. Opcionalmente, en este caso, el primer vector de confianza enviado al primer elemento de red puede incluir la clave simétrica K_{RAF} .

G403: El primer elemento de red envía una segunda solicitud de certificación al UE.

Para obtener descripciones específicas del paso G403, hacer referencia a las descripciones relacionadas del paso C406. Los detalles no se describen de nuevo en la presente.

G404: El UE determina la primera información de certificación.

Para obtener descripciones específicas del paso G404, hacer referencia a las descripciones relacionadas del paso C407. Los detalles no se describen de nuevo en la presente.

G405: El UE envía la primera información de certificación al primer elemento de red.

Para obtener descripciones específicas del paso G405, hacer referencia a las descripciones relacionadas del paso C408. Los detalles no se describen de nuevo en la presente.

G406: El primer elemento de red compara X_{att} y X_{att}' , y genera un primer resultado de certificación de confianza.

Específicamente, para obtener descripciones específicas de que el primer elemento de red compara X_{att} y X_{att}' , y genera el primer resultado de certificación de confianza, hacer referencia a las descripciones relacionadas del paso C409. Los detalles no se describen de nuevo en la presente.

Si X_{att} y X_{att}' son iguales, es decir, el primer resultado de certificación de confianza indica que el UE es confiable, el primer elemento de red deriva una primera clave de anclaje con base en la clave simétrica K_{RAF} , y el primer elemento de red envía la primera clave de anclaje al segundo elemento de red. Además, el segundo elemento de red determina una tercera clave de anclaje. Opcionalmente, el segundo elemento de red determina la primera

clave de anclaje como la tercera clave de anclaje.

A continuación se describe específicamente la derivación de clave de una clave simétrica por el uso de un ejemplo en el que una cuarta clave derivada es una clave de autenticación.

5 Diferente de la figura 4A, en esta modalidad, un chip de SIM en el UE no se preconfigura con una clave raíz K_{TPM} utilizada para la certificación de confianza. Sin embargo, una tarjeta de SIM aún se preconfigura con una clave raíz K utilizada para la autenticación. Además, la clave raíz en la tarjeta de SIM se actualiza adicionalmente a un servidor de recursos de un operador a través de un canal seguro. En esta modalidad, una clave simétrica
10 K_{RAF} que se va a utilizar por un primer elemento de red se deriva con base en la clave raíz K , y después de que la certificación de confianza del UE tiene éxito, una clave de autenticación K_{AUSF} que se va a utilizar por un elemento de red de autenticación se deriva con base en la clave simétrica K_{RAF} .

15 La figura 4H es un diagrama de otra arquitectura de clave de acuerdo con una modalidad de esta solicitud. Tanto un lado de red como un lado de UE realizan la derivación de clave con base en la arquitectura de clave en la figura 4H.

A continuación se describe un proceso de certificación de confianza de UE.

20 La figura 4I es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

I401: El UE envía una solicitud de registro a un segundo elemento de red, donde la solicitud incluye información de identificación del UE.

25 En esta modalidad, el segundo elemento de red puede ser un elemento de red de AMF, o el segundo elemento de red es un elemento de red en el que la AMF y una SEAF se despliegan conjuntamente.

I402: El segundo elemento de red envía una primera solicitud de certificación a un primer elemento de red, donde la solicitud incluye la información de identificación del UE.

30 Específicamente, el segundo elemento de red envía una solicitud de autenticación a un elemento de red de autenticación, y el elemento de red de autenticación envía una solicitud de vector de autenticación a un tercer elemento de red. Una secuencia de envío de la primera

solicitud de certificación y la solicitud de autenticación no se limita en particular.

5 El primer elemento de red obtiene un primer vector de confianza correspondiente con base en la información de identificación del UE. Para un proceso específico en el que el primer elemento de red obtiene el primer vector de confianza correspondiente con base en la información de identificación del UE, hacer referencia a las descripciones relacionadas que corresponden a la figura 4C. Se incluyen al menos dos métodos de obtención. Además, el tercer elemento de red envía un vector de autenticación generado y el primer vector de confianza al primer elemento de red.

I403: El primer elemento de red envía una segunda solicitud de certificación al UE.

10 I404: El UE determina la primera información de certificación.

I405: El UE envía la primera información de certificación al primer elemento de red.

Para obtener descripciones específicas del paso I405, hacer referencia a las descripciones relacionadas del paso C408. Los detalles no se describen de nuevo en la presente.

15 I406: El primer elemento de red compara X_{att} y X_{att}' , y genera un primer resultado de certificación de confianza. Si X_{att} y X_{att}' son iguales, es decir, el primer resultado de certificación de confianza indica que el UE es confiable, el primer elemento de red deriva una clave de autenticación K_{AUSF} con base en una clave simétrica K_{RAF} .

20 Para obtener descripciones específicas del paso I403 al paso I406, hacer referencia a las descripciones relacionadas del paso C407 al paso C409. Los detalles no se describen de nuevo en la presente.

I407: El primer elemento de red envía el vector de autenticación y la clave de autenticación al elemento de red de autenticación.

I408: El elemento de red de autenticación realiza la autenticación en el UE.

25 En esta modalidad, para un proceso específico en el que el elemento de red de autenticación realiza la autenticación en el UE, se hace referencia a la descripción en la figura 2C. Los detalles no se describen de nuevo en la presente.

I409: El elemento de red de autenticación compara RES y RES' , y cuando se entera,

a través de la comparación, de que RES y RES' son la mismas, el elemento de red de autenticación deriva una tercera clave de anclaje con base en la clave de autenticación K_{AUSF} , y envía la tercera clave de anclaje al segundo elemento de red.

En una posible modalidad, el método de certificación incluye además:

- 5 El primer elemento de red envía un segundo vector de confianza al segundo elemento de red o a un primer nodo. El segundo vector de confianza incluye la segunda información esperada, el segundo vector de confianza se utiliza por el segundo elemento de red o el primer nodo para realizar la certificación de confianza en la terminal, y la segunda información esperada incluye un segundo valor de verificación esperado.
- 10 En esta modalidad, el primer elemento de red envía el segundo vector de confianza al segundo elemento de red o al primer nodo, para entregar una capacidad de certificación de confianza al segundo elemento de red o al primer nodo. Opcionalmente, el segundo elemento de red o el primer nodo pueden iniciar la certificación de confianza del UE periódicamente o la certificación con base en otra política, para impedir que la información de certificación local
- 15 del UE se manipule.

- El primer nodo puede ser un dispositivo de red de acceso. Además, opcionalmente, esta modalidad puede ser independiente del método mostrado en la figura 3, es decir, no depende del primer resultado de certificación de confianza del UE. El segundo elemento de red o el primer nodo pueden iniciar la certificación de confianza del UE con base en una
- 20 situación real después de obtener el segundo vector de confianza. Opcionalmente, si el primer resultado de certificación de confianza indica que el UE es confiable, el primer elemento de red envía el segundo vector de confianza al segundo elemento de red o al primer nodo.

- Un proceso en el que el segundo elemento de red o el primer nodo realiza la certificación de confianza en el UE es similar a ese del primer elemento de red, e incluye: El
- 25 segundo elemento de red o el primer nodo recibe la segunda información de certificación del UE, y obtiene un segundo resultado de certificación de confianza de la terminal con base en la segunda información de certificación y la segunda información esperada. Opcionalmente, el segundo elemento de red o el primer nodo pueden enviar el segundo resultado de certificación de confianza al UE.

- 30 Por ejemplo, el segundo elemento de red o el primer nodo realiza la certificación de confianza con base en la segunda información de certificación de la terminal y la segunda

información esperada. La segunda información de certificación incluye un segundo valor de verificación, el segundo valor de verificación se obtiene al procesar un segundo número aleatorio y la información de certificación local de la terminal por el uso de una quinta clave derivada, y la quinta clave derivada se deriva de la clave simétrica. Para obtener un método específico para obtener el segundo valor de verificación, hacer referencia al método para obtener un primer valor de verificación. Los detalles no se describen de nuevo en la presente. El segundo valor de verificación esperado se obtiene al procesar el segundo número aleatorio y la segunda información de certificación esperada al usar la quinta clave derivada, y la segunda información de certificación esperada es la misma que la primera información de certificación esperada. Cuando se realiza la certificación de confianza en la terminal, el segundo elemento de red o el primer nodo se pueden enterar, a través de la comparación, de si el segundo valor de verificación es el mismo que el segundo valor de verificación esperado. La terminal es confiable si el segundo valor de verificación es el mismo que el segundo valor de verificación esperado; o la terminal no es confiable si el segundo valor de verificación es diferente del segundo valor de verificación esperado.

Por ejemplo, la segunda información esperada incluye además la segunda información de certificación esperada. Por ejemplo, la segunda información de certificación incluye además la información de certificación local de la terminal. En esta solicitud, cuando el segundo valor de verificación es el mismo que el segundo valor de verificación esperado, y la información de certificación local es la misma que la segunda información de certificación esperada, el segundo elemento de red o el primer nodo determina que la terminal es confiable; o cuando el segundo valor de verificación es diferente del segundo valor de verificación esperado, y/o la información de certificación local es diferente de la segunda información de certificación esperada, la terminal no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el segundo valor de verificación y el segundo valor de verificación esperado, y la información de certificación local y la segunda información de certificación esperada son las mismas, para garantizar una mayor fiabilidad del resultado de certificación de confianza de la terminal.

Por ejemplo, el segundo vector de confianza incluye además la quinta clave derivada.

Específicamente, la quinta clave derivada es una clave que se deriva por el lado de red y que se va a utilizar por el segundo elemento de red o el primer nodo. El UE también deriva la quinta clave derivada de la clave simétrica con base en un algoritmo de derivación de clave igual que ese en el lado de red, y el UE y el segundo elemento de red o el primer

nodo pueden realizar la certificación de confianza con base en la quinta clave derivada. Una quinta clave derivada que se va a utilizar por el primer nodo se deriva con base en una quinta clave derivada que se va a utilizar por el segundo elemento de red, y la quinta clave derivada que se va a utilizar por el segundo elemento de red se deriva con base en la clave simétrica.

- 5 En esta modalidad, cuando el primer elemento de red no completa un primer tiempo de certificación de confianza del UE, el segundo elemento de red o el primer nodo pueden solicitar el segundo vector de confianza del tercer elemento de red al utilizar el primer elemento de red, o el segundo elemento de red o el primer nodo solicita directamente el segundo vector de confianza del tercer elemento de red.
- 10 Opcionalmente, después de que el primer elemento de red completa la primera vez de certificación de confianza del UE, el primer elemento de red puede derivar alternativamente directamente la quinta clave derivada con base en la clave simétrica. Además, opcionalmente, debido a que la primera información de certificación esperada es la segunda información de certificación esperada, el primer elemento de red puede generar el segundo número aleatorio,
- 15 y entonces procesar la segunda información de certificación esperada y el segundo número aleatorio con base en la quinta clave derivada para obtener el segundo valor de verificación esperado. De esta manera, el primer elemento de red puede obtener el segundo vector de confianza.
- Al igual que el primer número aleatorio, el segundo número aleatorio puede ser un
- 20 número aleatorio que se genera por el primer elemento de red o el tercer elemento de red y que corresponde a la información de identificación del UE, es decir, el primer elemento de red o el tercer elemento de red genera un segundo número aleatorio para cada tiempo de certificación de confianza del UE. El primer elemento de red o el tercer elemento de red proporciona el segundo número aleatorio al UE de una manera de unidifusión o difusión.
- 25 Opcionalmente, cuando se verifica el segundo valor de verificación esperado, el segundo elemento de red o el primer nodo pueden procesar el segundo número aleatorio y la segunda información de certificación esperada con base en la quinta clave derivada para obtener el segundo valor de verificación esperado, y entonces verificar el segundo valor de verificación esperado con base en el segundo valor de verificación esperado.
- 30 Por ejemplo, la segunda información de certificación puede incluir además el segundo número aleatorio, para indicar que el segundo valor de verificación corresponde al segundo número aleatorio, en otras palabras, el segundo valor de verificación se genera con base en

el segundo número aleatorio. De manera similar, la segunda información esperada puede incluir además el segundo número aleatorio, para indicar que el segundo valor de verificación esperado corresponde al segundo número aleatorio, en otras palabras, el segundo valor de verificación esperado se genera con base en el segundo número aleatorio. Si la segunda información de certificación corresponde a la segunda información esperada se puede determinar al enterarse, a través de la comparación, de si el segundo número aleatorio en la segunda información de certificación es el mismo que el segundo número aleatorio en la segunda información esperada. Además, cuando el segundo número aleatorio en la segunda información de certificación es el mismo que el segundo número aleatorio en la segunda información esperada, el segundo valor de verificación es el mismo que el segundo valor de verificación esperado, y la información de certificación local es la misma que la segunda información de certificación esperada, el segundo elemento de red o el primer nodo determina que la terminal es confiable; o cuando el segundo número aleatorio en la segunda información de certificación es diferente del segundo número aleatorio en la segunda información esperada, y/o el segundo valor de verificación es diferente del segundo valor de verificación esperado, y/o la información de certificación local es diferente de la segunda información de certificación esperada, la terminal no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los tres grupos de parámetros, es decir, el segundo valor de verificación y el segundo valor de verificación esperado, la información de certificación local y la segunda información de certificación esperada, y el segundo número aleatorio en la segunda información de certificación y el segundo número aleatorio en la segunda información esperada son los mismos, para mejorar además la fiabilidad del resultado de certificación de confianza de la terminal.

En una posible modalidad, el método de certificación incluye además:

El primer elemento de red recibe el segundo vector de confianza del tercer elemento de red.

En esta modalidad, cuando el primer elemento de red no completa la primera vez de certificación de confianza del UE, el primer elemento de red puede solicitar el segundo vector de confianza del tercer elemento de red, y después de generar el segundo vector de confianza, el tercer elemento de red envía el segundo vector de confianza al primer elemento de red.

A continuación se describe específicamente, por el uso de un ejemplo en el que un primer nodo es un dispositivo de red de acceso, un proceso en el que el primer nodo realiza la certificación de confianza en el UE con base en un segundo vector de confianza.

En esta modalidad, lo mismo que en la figura 4A, una clave raíz K utilizada para la autenticación y una clave raíz K_{TPM} utilizada para la certificación de confianza se preestablecen en una tarjeta de SIM del UE. En una etapa de producción, un fabricante de tarjeta de SIM preestablece una función de TPM en la tarjeta de SIM, y actualiza la clave raíz K_{TPM} en la tarjeta de SIM a un servidor de recursos 402 de un operador a través de un canal seguro.

Como se muestra en la figura 4B, en esta modalidad, tanto un lado de red como un lado de UE realizan la derivación de clave con base en la arquitectura de clave en la figura 4B. Una clave $K_{\text{gNB-RA}}$ que se va a utilizar por un dispositivo de red de acceso se deriva con base en una clave $K_{\text{AMF-RA}}$ que se va a utilizar por un elemento de red de AMF.

A continuación se describe un proceso de certificación de confianza de UE.

La figura 4J es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

J401: Un primer elemento de red envía una solicitud de vector de confianza a un tercer elemento de red, donde la solicitud incluye información de identificación del UE.

Específicamente, la solicitud de vector de confianza se utiliza para solicitar un quinto vector de confianza, y el quinto vector de confianza incluye una clave $K_{\text{AMF-RA}}$, segunda información de certificación esperada, y un segundo valor de verificación esperado. En esta modalidad, se usa un ejemplo en el que el primer elemento de red obtiene el quinto vector de confianza del tercer elemento de red. En este caso, el tercer elemento de red realiza la derivación de clave para obtener la clave $K_{\text{AMF-RA}}$, y procesa la segunda información de certificación esperada y un segundo número aleatorio por el uso de la clave $K_{\text{AMF-RA}}$ para obtener el segundo valor de verificación esperado. El segundo número aleatorio puede ser un número aleatorio que se genera por el tercer elemento de red y que corresponde a la información de identificación del UE, o el segundo número aleatorio es un número aleatorio común que se transmite por el tercer elemento de red a una pluralidad de UE por adelantado. La pluralidad de UE son dos o más UE, y la pluralidad de UE incluye el UE en esta modalidad.

El tercer elemento de red retorna el quinto vector de confianza al primer elemento de red.

En esta modalidad, el primer elemento de red puede ser un elemento de red de RAF,

y el tercer elemento de red puede ser un elemento de red de TPMF. Opcionalmente, un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Opcionalmente, el elemento de red de TPMF y el elemento de red de RAF se despliegan conjuntamente.

- 5 J402: El primer elemento de red envía el quinto vector de confianza a un elemento de red de AMF.

El elemento de red de AMF obtiene un segundo vector de confianza con base en el quinto vector de confianza.

- 10 Específicamente, el elemento de red de AMF deriva una clave K_{gNB-RA} con base en la clave K_{AMF-RA} , y el segundo vector de confianza incluye la segunda información esperada. Además, el segundo vector de confianza puede incluir además la clave K_{gNB-RA} .

J403: El elemento de red de AMF envía el segundo vector de confianza a un primer nodo. El primer nodo es un dispositivo de red de acceso.

J404: El primer nodo envía una cuarta solicitud de certificación al UE.

- 15 Específicamente, la cuarta solicitud de certificación se utiliza para activar el UE para determinar la segunda información de certificación. El primer nodo puede enviar periódicamente la cuarta solicitud de certificación al UE, o el primer nodo envía la cuarta solicitud de certificación al UE con base en otra política. La otra política es, por ejemplo, enviar la cuarta solicitud de certificación al UE después de recibir una solicitud de registro del UE o
20 después de que el UE solicite un servicio.

- Cuando el segundo número aleatorio es un número aleatorio que se genera por el tercer elemento de red y que corresponde a la información de identificación del UE, la cuarta solicitud de certificación incluye el segundo número aleatorio. Cuando el segundo número aleatorio es un número aleatorio común que se transmite por el tercer elemento de red a la
25 pluralidad de UE por adelantado, el UE tiene el segundo número aleatorio, y la cuarta solicitud de certificación no necesita portar el segundo número aleatorio, y sólo se utiliza para activar el UE para determinar la segunda información de certificación.

J405: El UE determina la segunda información de certificación.

- 30 Específicamente, un lado de UE también deriva la clave K_{gNB-RA} , y el UE procesa la información de certificación local y el segundo número aleatorio con base en la clave K_{gNB-RA}

para obtener un segundo valor de verificación. De manera similar a la primera información de certificación, la segunda información de certificación incluye el segundo valor de verificación. Para otro ejemplo, la segunda información de certificación incluye además la información de certificación local. Por ejemplo, la segunda información de certificación es un valor de combinación de la información de certificación local y el segundo valor de verificación, y la segunda información de certificación se puede obtener a través del empalme en una secuencia de la información de certificación local y el segundo valor de verificación. Opcionalmente, la segunda información de certificación incluye además el segundo número aleatorio. Por ejemplo, la segunda información de certificación es un valor de combinación del segundo número aleatorio, la información de certificación local, y el segundo valor de verificación, y la segunda información de certificación se puede obtener a través del empalme en una secuencia del segundo número aleatorio, la información de certificación local, y el segundo valor de verificación.

J406: El UE envía una cuarta respuesta de certificación al primer nodo. La cuarta respuesta de certificación incluye la segunda información de certificación. Opcionalmente, la cuarta respuesta de certificación puede incluir además el segundo número aleatorio y/o la información de certificación local.

J407: El primer nodo determina un segundo resultado de certificación de confianza con base en la segunda información de certificación y la segunda información esperada.

Para obtener descripciones específicas del paso J407, hacer referencia a las descripciones del paso C409. Los detalles no se describen de nuevo en la presente.

J408: El primer nodo retroalimenta el segundo resultado de certificación de confianza al UE.

Opcionalmente, el primer nodo retroalimenta el segundo resultado de certificación de confianza al primer elemento de red.

Específicamente, el primer nodo retroalimenta el segundo resultado de certificación de confianza al primer elemento de red por el uso de AMF, tal que el primer elemento de red se entere de un resultado de certificación de confianza del UE desde el primer nodo, y el primer nodo endosa la información de certificación local del UE.

Como se muestra en la figura 4J, cuando el segundo elemento de red realiza la certificación de confianza en el UE con base en el segundo vector de confianza, por ejemplo,

el segundo elemento de red es una AMF, el quinto vector de confianza es el segundo vector de confianza. Después de que el elemento de red de AMF recibe el segundo vector de confianza, el elemento de red de AMF envía directamente la cuarta solicitud de certificación al UE por el uso del dispositivo de red de acceso. El UE retorna la cuarta respuesta de
5 certificación al elemento de red de AMF, y el elemento de red de AMF obtiene el segundo resultado de certificación de confianza con base en la cuarta respuesta de certificación.

En una posible modalidad, el método de certificación incluye además:

El primer elemento de red envía un tercer vector de confianza al segundo elemento de red o a un primer nodo. El tercer vector de confianza incluye una quinta clave derivada y la
10 segunda información de certificación esperada, el tercer vector de confianza se utiliza por el segundo elemento de red o el primer nodo para realizar la certificación de confianza en una terminal, y la quinta clave derivada se deriva de una clave simétrica.

En esta modalidad, el primer elemento de red envía el tercer vector de confianza al segundo elemento de red o al primer nodo, para entregar una capacidad de certificación de
15 confianza al segundo elemento de red o al primer nodo. Opcionalmente, el segundo elemento de red o el primer nodo pueden iniciar la certificación de confianza del UE periódicamente o la certificación con base en otra política, para impedir que la información de certificación local del UE se manipule. La segunda información de certificación esperada es la primera información de certificación esperada anterior. Diferente de la modalidad anterior que
20 corresponde al segundo vector de confianza, en esta modalidad, el segundo elemento de red o el primer nodo genera el segundo número aleatorio que corresponde a la información de identificación del UE, y entonces el segundo elemento de red o el primer nodo procesa el segundo número aleatorio y la segunda información de certificación esperada con base en la quinta clave derivada para obtener el segundo valor de verificación esperado. El segundo
25 elemento de red o el primer nodo pueden realizar la certificación de confianza en el UE con base en el segundo número aleatorio, la segunda información de certificación esperada, y el segundo valor de verificación esperado, para obtener el segundo resultado de certificación de confianza del UE. Para detalles relacionados en esta modalidad, se hace referencia a la modalidad anterior que corresponde al segundo vector de confianza.

Opcionalmente, esta modalidad puede ser independiente del método mostrado en la
30 figura 3, es decir, no depende del primer resultado de certificación de confianza del UE. El segundo elemento de red o el primer nodo pueden iniciar la certificación de confianza del UE con base en una situación real después de obtener el tercer vector de confianza.

Opcionalmente, si el primer resultado de certificación de confianza indica que el UE es confiable, el primer elemento de red envía el tercer vector de confianza al segundo elemento de red o al primer nodo.

5 Específicamente, la quinta clave derivada es una clave que se deriva por un lado de red y que se va a utilizar por el segundo elemento de red o el primer nodo. El UE también deriva la quinta clave derivada de la clave simétrica con base en un algoritmo de derivación de clave igual que ese en el lado de red, y el UE y el segundo elemento de red o el primer nodo pueden realizar la certificación de confianza con base en la quinta clave derivada.

10 En esta modalidad, cuando el primer elemento de red no completa un primer tiempo de certificación de confianza del UE, el segundo elemento de red o el primer nodo pueden solicitar el tercer vector de confianza del tercer elemento de red al utilizar el primer elemento de red, o el segundo elemento de red o el primer nodo solicita directamente el tercer vector de confianza del tercer elemento de red.

15 Opcionalmente, después de que el primer elemento de red completa la primera vez de certificación de confianza del UE, el primer elemento de red puede derivar alternativamente directamente la quinta clave derivada con base en la clave simétrica. Además, opcionalmente, debido a que la primera información de certificación esperada es la segunda información de certificación esperada, el primer elemento de red puede generar el segundo número aleatorio, y entonces procesar la segunda información de certificación esperada y el segundo número
20 aleatorio con base en la quinta clave derivada para obtener el segundo valor de verificación esperado. De esta manera, el primer elemento de red puede obtener el tercer vector de confianza.

25 Un proceso en el que el segundo elemento de red o el primer nodo realiza la certificación de confianza en el UE es similar a ese del primer elemento de red, e incluye: El segundo elemento de red o el primer nodo recibe la segunda información de certificación del UE, y obtiene un segundo resultado de certificación de confianza de la terminal con base en la segunda información de certificación y la segunda información esperada. Opcionalmente, el segundo elemento de red o el primer nodo pueden enviar el segundo resultado de certificación de confianza al UE.

30 En una posible modalidad, el método de certificación incluye además:

El primer elemento de red recibe el tercer vector de confianza del tercer elemento de

red.

En esta modalidad, cuando el primer elemento de red no completa la primera vez de certificación de confianza del UE, el primer elemento de red puede solicitar el tercer vector de confianza del tercer elemento de red, y después de generar el tercer vector de confianza, el tercer elemento de red envía el tercer vector de confianza al primer elemento de red.

A continuación se describe específicamente, por el uso de un ejemplo en el que un primer nodo es un dispositivo de red de acceso, un proceso en el que el primer nodo realiza la certificación de confianza en el UE con base en un tercer vector de confianza.

En esta modalidad, lo mismo que en la figura 4A, una clave raíz K utilizada para la autenticación y una clave raíz K_{TPM} utilizada para la certificación de confianza se preestablecen en una tarjeta de SIM del UE. En una etapa de producción, un fabricante de tarjeta de SIM preestablece una función de TPM en la tarjeta de SIM, y actualiza la clave raíz K_{TPM} en la tarjeta de SIM a un servidor de recursos 402 de un operador a través de un canal seguro.

Como se muestra en la figura 4B, en esta modalidad, tanto un lado de red como un lado de UE realizan la derivación de clave con base en la arquitectura de clave en la figura 4B. Una clave $K_{\text{gNB-RA}}$ que se va a utilizar por un dispositivo de red de acceso se deriva con base en una clave $K_{\text{AMF-RA}}$ que se va a utilizar por un elemento de red de AMF.

A continuación se describe un proceso de certificación de confianza de UE.

La figura 4K es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

K401: Un primer elemento de red envía una solicitud de vector de confianza a un tercer elemento de red, donde la solicitud incluye información de identificación del UE.

Específicamente, la solicitud de vector de confianza se utiliza para solicitar un sexto vector de confianza, y el sexto vector de confianza incluye una clave $K_{\text{AMF-RA}}$ y segunda información de certificación esperada. En esta modalidad, se usa un ejemplo en el que el primer elemento de red obtiene el sexto vector de confianza del tercer elemento de red. En este caso, el tercer elemento de red realiza la derivación de clave para obtener la clave $K_{\text{AMF-RA}}$. El tercer elemento de red retorna el sexto vector de confianza al primer elemento de red.

En esta modalidad, el primer elemento de red puede ser un elemento de red de RAF, y el tercer elemento de red puede ser un elemento de red de TPMF. Opcionalmente, un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Opcionalmente, el elemento de red de TPMF y el elemento de red de RAF se despliegan conjuntamente.

K402: El primer elemento de red envía el sexto vector de confianza a un elemento de red de AMF.

K403: El elemento de red de AMF envía un tercer vector de confianza a un primer nodo. El primer nodo es un dispositivo de red de acceso.

10 El elemento de red de AMF obtiene el tercer vector de confianza con base en el sexto vector de confianza. Específicamente, el elemento de red de AMF deriva una clave K_{gNB-RA} con base en la clave K_{AMF-RA} , y el tercer vector de confianza incluye la clave K_{gNB-RA} y la segunda información de certificación esperada.

K404: El primer nodo envía una cuarta solicitud de certificación al UE.

15 Específicamente, la cuarta solicitud de certificación se utiliza para activar el UE para determinar la segunda información de certificación, y la cuarta solicitud de certificación incluye un segundo número aleatorio. El primer nodo genera un segundo número aleatorio que corresponde a la información de identificación del UE. El primer nodo procesa el segundo número aleatorio y la segunda información de certificación esperada con base en la clave

20 K_{gNB-RA} para obtener un segundo valor de verificación esperado. El primer nodo puede enviar periódicamente la cuarta solicitud de certificación al UE, o el primer nodo envía la cuarta solicitud de certificación al UE con base en otra política. La otra política es, por ejemplo, enviar la cuarta solicitud de certificación al UE después de recibir una solicitud de registro del UE o después de que el UE solicite un servicio.

25 K405: El UE determina la segunda información de certificación.

K406: El UE envía una cuarta respuesta de certificación al primer nodo. La cuarta respuesta de certificación incluye la segunda información de certificación. Opcionalmente, la cuarta respuesta de certificación puede incluir además el segundo número aleatorio y/o información de certificación local.

30 K407: El primer nodo determina un segundo resultado de certificación de confianza

con base en la segunda información de certificación y la segunda información esperada.

Para obtener descripciones específicas del paso K407, hacer referencia a las descripciones del paso C409. Los detalles no se describen de nuevo en la presente.

5 K408: El primer nodo retroalimenta el segundo resultado de certificación de confianza al UE.

Opcionalmente, el primer nodo retroalimenta el segundo resultado de certificación de confianza al primer elemento de red.

10 Como se muestra en la figura 4K, cuando el primer nodo y el elemento de red de AMF en la figura 4K se reemplazan con el elemento de red de AMF, el sexto vector de confianza es el tercer vector de confianza. Después de que el elemento de red de AMF recibe el tercer vector de confianza, el elemento de red de AMF envía directamente la cuarta solicitud de certificación al UE por el uso del dispositivo de red de acceso. Un procedimiento de procesamiento posterior es el mismo que cuando el primer nodo es un dispositivo de red de acceso. Los detalles no se describen de nuevo en la presente.

15 Una modalidad de esta solicitud proporciona además un método de certificación, para realizar una certificación de confianza en un tercer nodo. El tercer nodo puede ser un dispositivo de red de acceso o un elemento de red central.

La figura 5 es un diagrama de flujo de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

20 501: Un segundo nodo envía una tercera solicitud de certificación a un tercer nodo.

Por consiguiente, el tercer nodo recibe la tercera solicitud de certificación del segundo nodo.

Específicamente, la tercera solicitud de certificación se utiliza para activar el tercer nodo para determinar la tercera información de certificación.

25 El segundo nodo puede ser un elemento de red de RAF, un elemento de red de OAM, o un elemento de red de NRF. Cuando el segundo nodo es un elemento de red de RAF, y el tercer nodo es un elemento de red de núcleo, el tercer nodo es un elemento de red de núcleo distinto del elemento de red de RAF. Cuando el segundo nodo es un elemento de red de OAM, y el tercer nodo es un elemento de red de núcleo, el tercer nodo es un elemento de red de

núcleo distinto del elemento de red de OAM. Cuando el segundo nodo es un elemento de red de NRF, y el tercer nodo es un elemento de red de núcleo, el tercer nodo es un elemento de red de núcleo distinto del elemento de red de NRF.

5 502: El tercer nodo determina la tercera información de certificación, y el tercer nodo determina la tercera información de certificación en respuesta a la tercera solicitud de certificación.

503: El tercer nodo envía la tercera información de certificación al segundo nodo.

Por consiguiente, el segundo nodo recibe la tercera información de certificación del tercer nodo.

10 504: El segundo nodo obtiene un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

Específicamente, el resultado de certificación de confianza indica que el tercer nodo es confiable o no confiable.

15 En esta modalidad, el segundo nodo puede determinar el resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación del tercer nodo y la tercera información esperada, para implementar la certificación de confianza del tercer nodo.

En una posible modalidad, como se muestra en la figura 5, el método de certificación incluye además:

20 505: El segundo nodo envía el resultado de certificación de confianza al tercer nodo.

Por consiguiente, el tercer nodo recibe el resultado de certificación de confianza del tercer nodo del segundo nodo.

25 Se puede enterar de que, en esta modalidad, el segundo nodo retroalimenta el resultado de certificación de confianza del tercer nodo al tercer nodo, tal que el tercer nodo obtenga el resultado de certificación de confianza del tercer nodo.

En una posible modalidad, la tercera información de certificación en el paso 502 incluye un tercer valor de verificación, el tercer valor de verificación se obtiene al procesar un tercer número aleatorio e información de certificación local por el uso de una clave simétrica, la clave

simétrica es una clave utilizada para la certificación de confianza, y la clave simétrica significa que el segundo nodo y el tercer nodo tienen una misma clave utilizada para la certificación de confianza. La tercera información esperada incluye un tercer valor de verificación esperado. En el paso 504, el segundo nodo se entera, a través de la comparación, de si el tercer valor de verificación esperado es el mismo que el tercer valor de verificación, y cuando se entera, a través de la comparación, de que el tercer valor de verificación esperado es el mismo que el tercer valor de verificación, el resultado de certificación de confianza del tercer nodo es que el tercer nodo es confiable; o cuando se entera, a través de la comparación, de que el tercer valor de verificación esperado es diferente del tercer valor de verificación, el resultado de certificación de confianza del tercer nodo es que el tercer nodo no es confiable.

En una posible modalidad, la tercera información de certificación en el paso 502 incluye además la información de certificación local del tercer nodo. La tercera información esperada incluye además la tercera información de certificación esperada. En el paso 504, el segundo nodo se entera, a través de la comparación, de si la tercera información de certificación esperada es la misma que la información de certificación local del tercer nodo, y se entera, a través de la comparación, de si el tercer valor de verificación esperado es el mismo que el tercer valor de verificación, y cuando se entera, a través de la comparación, de que la tercera información de certificación esperada es la misma que la información de certificación local del tercer nodo, y el tercer valor de verificación esperado es el mismo que el tercer valor de verificación, el resultado de certificación de confianza del tercer nodo es que el tercer nodo es confiable; o cuando se entera, a través de la comparación, de que la tercera información de certificación esperada es diferente de la información de certificación local del tercer nodo, y/o el tercer valor de verificación esperado es diferente del tercer valor de verificación, el resultado de certificación de confianza del tercer nodo es que el tercer nodo no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los dos grupos de parámetros, es decir, el tercer valor de verificación y el tercer valor de verificación esperado, y la información de certificación local del tercer nodo y la tercera información de certificación esperada son las mismas, para garantizar una mayor fiabilidad del resultado de certificación de confianza del tercer nodo.

Por ejemplo, la tercera información de certificación puede incluir además el tercer número aleatorio, para indicar que el tercer valor de verificación corresponde al tercer número aleatorio. De manera similar, la tercera información esperada puede incluir además el tercer número aleatorio, para indicar que la tercera información de certificación esperada y el tercer valor de verificación esperado corresponden al tercer número aleatorio. En el paso 504, el

segundo nodo se entera además, a través de la comparación, de si el tercer número aleatorio en la tercera información de certificación es el mismo que el tercer número aleatorio en la tercera información esperada. Cuando se entera, a través de la comparación, de que la tercera información de certificación esperada es la misma que la información de certificación local del tercer nodo, el tercer valor de verificación esperado es el mismo que el tercer valor de verificación, y el tercer número aleatorio en la tercera información de certificación es el mismo que el tercer número aleatorio en la tercera información esperada, el resultado de certificación de confianza del tercer nodo es que el tercer nodo es confiable; o cuando se entera, a través de la comparación, de que la tercera información de certificación esperada es diferente de la información de certificación local del tercer nodo, y/o el tercer valor de verificación esperado es diferente del tercer valor de verificación, y/o el tercer número aleatorio en la tercera información de certificación es diferente del tercer número aleatorio en la tercera información esperada, el resultado de certificación de confianza del tercer nodo es que el tercer nodo no es confiable. En esta solicitud, la verificación de confianza se realiza al verificar si los tres grupos de parámetros, es decir, el tercer valor de verificación y el tercer valor de verificación esperado, la información de certificación local del tercer nodo y la tercera información de certificación esperada, y el tercer número aleatorio en la tercera información de certificación y el tercer número aleatorio en la tercera información esperada son los mismos, para mejorar además la fiabilidad del resultado de certificación de confianza del tercer nodo.

En una posible modalidad, la clave simétrica es cualquiera de las siguientes:

Clave raíz utilizada para la certificación de confianza: Para ser específicos, el tercer nodo se preconfigura con la clave raíz especialmente utilizada para la certificación de confianza, y comparte de manera segura la clave raíz con un lado de red, tal que el tercer nodo y el segundo nodo realicen la certificación de confianza con base en la clave raíz.

Sexta clave derivada: La sexta clave derivada se deriva de la clave raíz utilizada para la certificación de confianza. Para ser específicos, el tercer nodo se preconfigura con la clave raíz especialmente utilizada para la certificación de confianza, y comparte de manera segura la clave raíz con el lado de red. Una terminal y el lado de red (por ejemplo, el segundo nodo o el tercer elemento de red) derivan la sexta clave derivada con base en un mismo algoritmo de derivación, tal que el tercer nodo y el segundo nodo realicen la certificación de confianza con base en la sexta clave derivada.

En una posible modalidad, en el método de certificación, el segundo nodo se puede desplegar conjuntamente con el tercer elemento de red, y el tercer elemento de red es un

elemento de red de TPMF. Opcionalmente, un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Opcionalmente, el elemento de red de TPMF y el elemento de red de RAF se despliegan conjuntamente. En este caso, el segundo nodo almacena la tercera información de certificación esperada del tercer nodo, y el segundo nodo puede generar el tercer número aleatorio, y entonces procesar el tercer número aleatorio y la tercera información de certificación esperada con base en la clave simétrica para obtener el tercer valor de verificación esperado. De esta manera, el segundo nodo puede obtener la tercera información esperada, y el segundo nodo puede iniciar la certificación de confianza del tercer nodo con base en un requisito real, es decir, enviar la tercera solicitud de certificación al tercer nodo. La tercera solicitud de certificación incluye el tercer número aleatorio.

En una posible modalidad, cuando el segundo nodo y el tercer elemento de red se despliegan por separado, el método de certificación incluye además los siguientes pasos:

El segundo nodo envía una solicitud de vector de confianza al tercer elemento de red. La solicitud de vector de confianza incluye información de identificación del tercer nodo.

El segundo nodo recibe un cuarto vector de confianza del tercer elemento de red. El cuarto vector de confianza incluye la tercera información esperada.

Específicamente, el tercer elemento de red puede ser un elemento de red de TPMF. Opcionalmente, un elemento de red de UDM y el elemento de red de TPMF se despliegan conjuntamente. Opcionalmente, el elemento de red de TPMF y el elemento de red de RAF se despliegan conjuntamente. Por ejemplo, el tercer elemento de red almacena la tercera información de certificación esperada del tercer nodo, y el tercer elemento de red puede generar el tercer número aleatorio, y entonces procesar el tercer número aleatorio y la tercera información de certificación esperada con base en la clave simétrica para obtener el tercer valor de verificación esperado. La tercera información esperada incluye el tercer valor de verificación esperado. Opcionalmente, la tercera información esperada incluye además la tercera información de certificación esperada. Opcionalmente, la tercera información esperada incluye además el tercer número aleatorio. Para otro ejemplo, el cuarto vector de confianza puede incluir además la clave simétrica.

A continuación se describe específicamente, por el uso de un ejemplo en el que un segundo nodo es un elemento de red de OAM y un tercer nodo es un dispositivo de red de acceso, un proceso en el que el elemento de red de OAM realiza la certificación de confianza

en el dispositivo de red de acceso.

La figura 6A es un diagrama de otro procedimiento de certificación de confianza de acuerdo con una modalidad de esta solicitud. De manera similar a UE, se usa un ejemplo en el que un chip de seguridad es un chip de TPM. En una etapa de producción de un dispositivo de red de acceso 601, una función de TPM y una clave raíz utilizadas para la certificación de confianza se preestablecen en el dispositivo de red de acceso, y la clave raíz se actualiza a un servidor de recursos 602 de un operador a través de un canal seguro. De esta manera, en un proceso posterior de uso del dispositivo de red de acceso 601, se puede realizar una certificación de confianza remota entre una red de operador 603 y el dispositivo de red de acceso 601 con base en la clave raíz. De manera alternativa, la red de operador 603 realiza la derivación de clave con base en la clave raíz K en el servidor de recursos 602 para obtener una sexta clave derivada, el dispositivo de red de acceso 601 realiza la derivación de clave con base en la clave raíz en el dispositivo de red de acceso 601 para obtener la sexta clave derivada, y se puede realizar una certificación de confianza remota entre la red de operador 603 y el dispositivo de red de acceso 601 con base en la sexta clave derivada.

A continuación se describe específicamente un proceso de certificación de confianza del dispositivo de red de acceso.

La figura 6B es un diagrama de flujo de interacción de otro método de certificación de acuerdo con una modalidad de esta solicitud. El método de certificación incluye los siguientes pasos.

B601: Un elemento de red de OAM envía una solicitud de vector de confianza a un tercer elemento de red, donde la solicitud incluye información de identificación del elemento de red de OAM.

B602: El tercer elemento de red obtiene un cuarto vector de confianza con base en la información de identificación del elemento de red de OAM.

Específicamente, se usa un ejemplo en el que el cuarto vector de confianza incluye la tercera información esperada, y la tercera información esperada incluye un tercer número aleatorio, la tercera información de certificación esperada, y un tercer valor de verificación esperado.

B603: El tercer elemento de red envía el cuarto vector de confianza al elemento de red de OAM.

B604: El elemento de red de OAM envía una tercera solicitud de certificación al dispositivo de red de acceso, donde la solicitud incluye el tercer número aleatorio.

B605: El dispositivo de red de acceso determina la tercera información de certificación.

5 Por ejemplo, la tercera información de certificación incluye el tercer número aleatorio, la información de certificación local del dispositivo de red de acceso, y un tercer valor de verificación.

B606: El dispositivo de red de acceso envía una tercera respuesta de certificación al elemento de red de OAM, donde la respuesta incluye la tercera información de certificación.

10 B607: El elemento de red de OAM compara la tercera información de certificación y la tercera información esperada, para obtener un resultado de certificación de confianza del dispositivo de red de acceso.

Por ejemplo, el elemento de red de OAM se entera, a través de la comparación, de si el tercer número aleatorio en la tercera información de certificación es el mismo que el tercer número aleatorio en la tercera información esperada; el elemento de red de OAM se entera, a través de la comparación, de si la tercera información de certificación esperada es la misma que la información de certificación local del dispositivo de red de acceso, y se entera, a través de la comparación, de si el tercer valor de verificación esperado es el mismo que el tercer valor de verificación; y cuando se entera, a través de la comparación, de que el tercer número aleatorio en la tercera información de certificación es el mismo que el tercer número aleatorio en la tercera información esperada, la tercera información de certificación esperada es la misma que la información de certificación local del dispositivo de red de acceso, y el tercer valor de verificación esperado es el mismo que el tercer valor de verificación, el resultado de certificación de confianza del dispositivo de red de acceso es que el dispositivo de red de acceso es confiable; o cuando se entera, a través de la comparación, de que el tercer número aleatorio en el tercer la información de certificación es diferente del tercer número aleatorio en la tercera información esperada, y/o la tercera información de certificación esperada no es la misma que la información de certificación local del dispositivo de red de acceso, y/o el tercer valor de verificación esperado es diferente del tercer valor de verificación, el resultado de certificación de confianza del dispositivo de red de acceso es que el dispositivo de red de acceso no es confiable.

B608: El elemento de red de OAM retorna el resultado de certificación de confianza al

dispositivo de red de acceso.

La figura 7, FIGURA 8, FIGURA 9, y la FIGURA 10 son cada uno un diagrama de una estructura de un posible aparato de acuerdo con una modalidad de esta solicitud. Los aparatos se pueden configurar para implementar funciones del primer elemento de red, la terminal, el segundo nodo, y el tercer nodo en las modalidades de método anteriores. Por lo tanto, también se pueden implementar los efectos beneficiosos en las modalidades de método anteriores. En esta modalidad de esta solicitud, el aparato puede ser un primer elemento de red, una terminal, un segundo nodo, y un tercer nodo, o puede ser un módulo (por ejemplo, un chip) utilizado en el primer elemento de red, la terminal, el segundo nodo, y el tercer nodo.

La figura 7 es un diagrama de una estructura de un primer elemento de red de acuerdo con una modalidad de esta solicitud. Un primer elemento de red 700 incluye un módulo de recepción 701 y un módulo de procesamiento 702. El primer elemento de red 700 se configura para implementar una función del primer elemento de red en la modalidad de método mostrada en la figura 3. De manera alternativa, el primer elemento de red 700 puede incluir un módulo configurado para implementar cualquier función u operación del primer elemento de red en la modalidad de método mostrada en la figura 3, y el módulo se puede implementar de manera completa o parcialmente al usar software, hardware, firmware, o cualquier combinación de los mismos.

Cuando el primer elemento de red 700 se configura para implementar la función del primer elemento de red en la modalidad de método mostrada en la figura 3, el módulo de recepción 701 se configura para recibir la primera información de certificación de una terminal. El módulo de procesamiento 702 se configura para obtener un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación y la primera información esperada.

La figura 8 es un diagrama de una estructura de una terminal de acuerdo con una modalidad de esta solicitud. Una terminal 800 incluye un módulo de determinación 801 y un módulo de envío 802. La terminal 800 se configura para implementar una función de la terminal en la modalidad de método mostrada en la figura 3. De manera alternativa, la terminal 800 puede incluir un módulo configurado para implementar cualquier función u operación de la terminal en la modalidad de método mostrada en la figura 3, y el módulo se puede implementar de manera completa o parcialmente al usar software, hardware, firmware, o cualquier combinación de los mismos.

Cuando la terminal 800 se configura para implementar la función de la terminal en la modalidad de método mostrada en la figura 3, el módulo de determinación 801 se configura para determinar la primera información de certificación. El módulo de envío 802 se configura para enviar la primera información de certificación a un primer elemento de red.

5 Por ejemplo, una modalidad de esta solicitud proporciona además un sistema de comunicación. El sistema incluye el primer elemento de red y el segundo elemento de red mostrado en la figura 7.

El segundo elemento de red se configura para enviar una primera solicitud de certificación al primer elemento de red. La primera solicitud de certificación incluye información
10 de identificación de una terminal.

El primer elemento de red 700 se configura para recibir la primera información de certificación de la terminal.

El primer elemento de red 700 se configura además para obtener un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación
15 y la primera información esperada.

La figura 9 es un diagrama de una estructura de un segundo nodo de acuerdo con una modalidad de esta solicitud. Un segundo nodo 900 incluye un módulo de envío 901, un módulo de recepción 902, y un módulo de determinación 903. El segundo nodo 900 se configura para implementar una función del segundo nodo en la modalidad de método mostrada en la figura
20 5. De manera alternativa, el segundo nodo 900 puede incluir un módulo configurado para implementar cualquier función u operación del segundo nodo en la modalidad de método mostrada en la figura 5, y el módulo se puede implementar de manera completa o parcialmente al usar software, hardware, firmware, o cualquier combinación de los mismos.

Cuando el segundo nodo 900 se configura para implementar la función del segundo
25 nodo en la modalidad de método mostrada en la figura 5, el módulo de envío 901 se configura para enviar una tercera solicitud de certificación a un tercer nodo. El módulo de recepción 902 se configura para recibir tercera información de certificación del tercer nodo. El módulo de determinación 903 se configura para obtener un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información
30 esperada.

La figura 10 es un diagrama de una estructura de un tercer nodo de acuerdo con una

modalidad de esta solicitud. Un tercer nodo 1000 incluye un módulo de recepción 1001 y un módulo de envío 1002. El tercer nodo 1000 se configura para implementar una función del tercer nodo en la modalidad de método mostrada en la figura 5. De manera alternativa, el tercer nodo 1000 puede incluir un módulo configurado para implementar cualquier función u
5 operación del tercer nodo en la modalidad de método mostrada en la figura 5, y el módulo se puede implementar de manera completa o parcialmente al usar software, hardware, firmware, o cualquier combinación de los mismos.

Cuando el tercer nodo 1000 se configura para implementar la función del tercer nodo en la modalidad de método mostrada en la figura 5, el módulo de recepción 1001 se configura
10 para recibir una tercera solicitud de certificación de un segundo nodo. El módulo de envío 1002 se configura para enviar la tercera información de certificación al segundo nodo. La tercera información de certificación incluye un tercer valor de verificación, el tercer valor de verificación se obtiene al procesar un tercer número aleatorio e información de certificación local del tercer nodo por el uso de una clave simétrica, y la clave simétrica es una clave
15 utilizada para la certificación de confianza.

Por ejemplo, una modalidad de esta solicitud proporciona además un sistema de comunicación. El sistema incluye el segundo nodo mostrado en la figura 9 y el tercer nodo mostrado en la figura 10.

La figura 11 es un diagrama de una estructura de un aparato de comunicación de
20 acuerdo con una modalidad de la presente solicitud.

El aparato de comunicación 1100 incluye una memoria 1101, un procesador 1102, una interfaz de comunicación 1104, y un bus 1103. La memoria 1101, el procesador 1102, y la interfaz de comunicación 1104 se conectan de manera comunicativa entre sí a través del bus 1103. Puede haber una o más memorias 1101, y puede haber uno o más procesadores 1102.

25 Por ejemplo, el aparato de comunicación 1100 puede ser un chip o un sistema de chip.

La memoria 1101 puede ser una memoria de sólo lectura (Read-Only Memory, ROM), un dispositivo de almacenamiento estático, un dispositivo de almacenamiento dinámico, o una memoria de acceso aleatorio (Random Access Memory, RAM). La memoria 1101 puede almacenar un programa. Cuando el programa almacenado en la memoria 1101 se ejecuta por
30 el procesador 1102, el procesador 1102 se configura para realizar los pasos del método de certificación en cualquiera de las modalidades anteriores.

El procesador 1102 puede ser una unidad de procesamiento central de propósito general (Central Processing Unit, CPU), un microprocesador, un circuito integrado de aplicación específica (application-specific integrated circuit, ASIC), una unidad de procesamiento de gráficos (graphics processing unit, GPU), o uno o más circuitos integrados, y se configura para ejecutar un programa relacionado, para implementar el método de certificación en cualquiera de las modalidades anteriores.

Alternativamente, el procesador 1102 puede ser un chip de circuito integrado, y tiene una capacidad de procesamiento de señal. En un proceso de implementación, los pasos del método de certificación en cualquiera de las modalidades anteriores de esta solicitud se pueden completar por el uso de un circuito lógico integrado de hardware en el procesador 1102 o por el uso de instrucciones en una forma de software. De manera alternativa, el procesador 1102 puede ser un procesador de propósito general, un procesador de señal digital (Digital Signal Processor, DSP), un circuito integrado de aplicación específica (ASIC), un arreglo de compuertas programables en el campo (Field Programmable Gate Array, FPGA) u otro dispositivo lógico programable, una compuerta discreta o un dispositivo lógico de transistor, o un componente de hardware discreto. Puede implementar o realizar los métodos, los pasos y los diagramas de bloques lógicos que se describen en las modalidades de esta solicitud. El procesador de propósito general puede ser un microprocesador, o el procesador puede ser cualquier procesador convencional o similares. Los pasos del método de certificación descritos con referencia a cualquiera de las modalidades de esta solicitud se pueden realizar y completar directamente por un procesador de decodificación de hardware, o se pueden realizar y completar al usar una combinación de hardware en el procesador de decodificación y un módulo de software. Un módulo de software puede ubicarse en un medio de almacenamiento maduro en la técnica, como una memoria de acceso aleatorio, una memoria flash, una memoria de sólo lectura, una memoria programable de sólo lectura, una memoria programable y eléctricamente borrable o un registro. El medio de almacenamiento se ubica en la memoria 1101, y el procesador 1102 lee información de la memoria 1101 y completa el método de certificación en cualquiera de las modalidades anteriores en combinación con el hardware del procesador 1102.

La interfaz de comunicación 1104 es un aparato de transceptor que incluye, pero no se limita a, un transceptor, para implementar la comunicación entre el aparato de comunicación 1100 y otro dispositivo o una red de comunicación. Por ejemplo, el aparato de comunicación 1100 puede obtener segundos datos a través de la interfaz de comunicación 1104.

El bus 1103 puede incluir una ruta para transmitir información entre varios componentes (por ejemplo, la memoria 1101, el procesador 1102 y la interfaz de comunicación 1104) del aparato de comunicación 1100.

5 Se debe observar que, aunque sólo la memoria, el procesador, y la interfaz de comunicación del aparato de comunicación 1100 mostrado en la figura 11 se muestran, en un proceso de implementación específico, una persona experta en la técnica debe entender que el aparato de comunicación 1100 puede incluir además otro componente necesario para el funcionamiento normal. Además, con base en un requisito específico, un experto en la técnica debe entender que el aparato de comunicación 1100 puede incluir además un componente
10 de hardware para implementar otra función adicional. Además, un experto en la técnica debe entender que el aparato de comunicación 1100 puede incluir sólo un componente necesario para implementar modalidades de esta solicitud, y no necesita incluir todos los componentes mostrados en la figura 11.

En las diversas modalidades proporcionadas en esta solicitud, debe entenderse que
15 el sistema, aparato y método descritos pueden implementarse de otras maneras. Por ejemplo, la modalidad del aparato descrito es meramente un ejemplo. Por ejemplo, la división en las unidades es una mera división de función lógica y puede ser otra división en la aplicación real. Por ejemplo, una pluralidad de unidades o componentes pueden combinarse o integrarse en otro sistema, o algunas características pueden ignorarse o no realizarse. Además, los
20 acoplamientos mutuos o acoplamientos visualizados o analizados o los acoplamientos directos o conexiones de comunicación pueden implementarse al utilizar algunas interfaces. Los acoplamientos indirectos o las conexiones de comunicación entre los aparatos o unidades pueden implementarse en formas electrónicas, mecánicas u otras.

Las unidades descritas como partes separadas pueden o pueden no estar físicamente
25 separadas, y las partes mostradas como unidades pueden o pueden no ser unidades físicas, se pueden ubicar en una posición, o se pueden distribuir en una pluralidad de unidades de red. Algunas o todas las unidades pueden seleccionarse con base en los requerimientos reales para lograr los objetivos de las soluciones de las modalidades.

Adicionalmente, las unidades funcionales en las modalidades de la presente solicitud
30 pueden integrarse en una unidad de procesamiento, cada una de las unidades puede existir físicamente sola, o dos o más unidades pueden integrarse en una unidad.

Todas o algunas de las modalidades anteriores pueden implementarse utilizando

software, hardware, firmware o cualquier combinación de los mismos. Cuando se utiliza software para implementar las modalidades, todas o una parte de las modalidades se pueden implementar en una forma de un producto de programa de computadora. El producto de programa de computadora incluye una o más instrucciones de computadora. Cuando las

5 instrucciones informáticas se cargan y ejecutan en la computadora, el procedimiento o funciones de acuerdo con las modalidades de esta solicitud se generan total o parcialmente. La computadora puede ser una computadora de propósito general, una computadora dedicada, una red informática u otros aparatos programables. Las instrucciones de computadora pueden almacenarse en un medio de almacenamiento legible por computadora

10 o pueden transmitirse desde un medio de almacenamiento legible por computadora a otro medio de almacenamiento legible por computadora. Por ejemplo, las instrucciones de computadora pueden transmitirse desde un sitio web, computadora, servidor o centro de datos a otro sitio web, computadora, servidor o centro de datos en una forma alámbrica (por ejemplo, un cable coaxial, una fibra óptica o una línea de suscriptor digital) o inalámbrica (por ejemplo,

15 infrarrojo, radio o microondas). El medio de almacenamiento legible por computadora puede ser cualquier medio utilizable y accesible por computadora o un dispositivo de almacenamiento de datos, por ejemplo, un servidor o un centro de datos, que integre uno o más medios utilizables. El medio utilizable puede ser un medio magnético (por ejemplo, un disco flexible, un disco duro, o una cinta magnética), un medio óptico (por ejemplo, un DVD),

20 un medio semiconductor (por ejemplo, una unidad de estado sólido), o similares.

Las descripciones anteriores son simplemente implementaciones específicas de esta solicitud, pero no se propone que limiten el alcance de protección de esta solicitud. Cualquier variación o reemplazo fácilmente descubierto por un experto en la técnica dentro del alcance técnico divulgado en esta solicitud caerá dentro del alcance de protección de esta solicitud.

25 Por lo tanto, el alcance de protección de esta solicitud estará sujeto al alcance de protección de las reivindicaciones.