

REIVINDICACIONES

1. Un método de certificación, caracterizado porque el método comprende:

recibir, por un primer elemento de red, la primera información de certificación de una terminal; y

5 obtener, por el primer elemento de red, un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación y la primera información esperada.

2. El método de conformidad con la reivindicación 1, caracterizado porque la primera información de certificación comprende un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación local de la terminal por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza.

3. El método de conformidad con la reivindicación 2, caracterizado porque la primera información de certificación comprende además la información de certificación local.

15 4. El método de conformidad con cualquiera de las reivindicaciones 1 a 3, caracterizado porque la primera información esperada comprende un primer valor de verificación esperado.

5. El método de conformidad con la reivindicación 4, caracterizado porque la primera información esperada comprende además la primera información de certificación esperada.

20 6. El método de conformidad con cualquiera de las reivindicaciones 2 a 5, caracterizado porque antes de recibir, por el primer elemento de red, la primera información de certificación de la terminal, el método comprende además:

recibir, por el primer elemento de red, una primera solicitud de certificación de un segundo elemento de red, en donde la primera solicitud de certificación comprende información de identificación de la terminal; y

enviar, por el primer elemento de red, una segunda solicitud de certificación a la terminal, en donde la segunda solicitud de certificación comprende el primer número aleatorio, y el primer número aleatorio corresponde a la información de identificación de la terminal.

7. El método de conformidad con cualquiera de las reivindicaciones 2 a 6, caracterizado porque el método además comprende:

5 obtener, por el primer elemento de red, un primer vector de confianza que corresponde a la información de identificación de la terminal, en donde el primer vector de confianza comprende la primera información esperada.

8. El método de conformidad con la reivindicación 7, caracterizado porque obtener, por el primer elemento de red, el primer vector de confianza que corresponde a la información de identificación de la terminal comprende:

10 enviar, por el primer elemento de red, una solicitud de vector de confianza a un tercer elemento de red, en donde la solicitud de vector de confianza comprende la información de identificación de la terminal; y

recibir, por el primer elemento de red, 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.

15 9. El método de conformidad con la reivindicación 7, caracterizado porque obtener, por el primer elemento de red, el primer vector de confianza que corresponde a la información de identificación de la terminal comprende:

recibir, por el primer elemento de red, el primer vector de confianza de un elemento de red de autenticación.

20 10. El método de conformidad con cualquiera de las reivindicaciones 7 a 9, caracterizado porque el primer vector de confianza comprende además la clave simétrica.

11. El método de conformidad con cualquiera de las reivindicaciones 2 a 10, caracterizado porque la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza;

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

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

una tercera clave derivada, en donde la tercera clave derivada se deriva de una clave

de autenticación.

12. El método de conformidad con cualquiera de las reivindicaciones 2 a 11, caracterizado porque el método además comprende:

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

13. El método de conformidad con cualquiera de las reivindicaciones 2 a 12, caracterizado porque el método además comprende:

10 enviar, por el primer elemento de red, un segundo vector de confianza al segundo elemento de red o un primer nodo, en donde el segundo vector de confianza comprende 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 comprende un segundo valor de verificación esperado.

15 14. El método de conformidad con la reivindicación 13, caracterizado porque el segundo vector de confianza comprende además una quinta clave derivada, y la quinta clave derivada se deriva de la clave simétrica.

15. El método de conformidad con la reivindicación 13 o 14, caracterizado porque el método además comprende:

20 recibir, por el primer elemento de red, el segundo vector de confianza del tercer elemento de red.

16. El método de conformidad con cualquiera de las reivindicaciones 2 a 12, caracterizado porque el método además comprende:

25 enviar, por el primer elemento de red, un tercer vector de confianza al segundo elemento de red o un primer nodo, en donde el tercer vector de confianza comprende 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.

17. El método de conformidad con la reivindicación 16, caracterizado porque el método

comprende además:

recibir, por el primer elemento de red, el tercer vector de confianza del tercer elemento de red.

5 18. El método de conformidad con cualquiera de las reivindicaciones 1 a 17, caracterizado porque el método comprende además:

enviar, por el primer elemento de red, el primer resultado de certificación de confianza a la terminal.

19. Un método de certificación, caracterizado porque el método comprende:

determinar, por una terminal, la primera información de certificación; y

10 enviar, por la terminal, la primera información de certificación a un primer elemento de red.

20. El método de conformidad con la reivindicación 19, caracterizado porque la primera información de certificación comprende un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación local de la terminal por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza.

21. El método de conformidad con la reivindicación 20, caracterizado porque la primera información de certificación comprende además la información de certificación local.

20 22. El método de conformidad con la reivindicación 20 o 21, caracterizado porque antes de determinar, por la terminal, la primera información de certificación, el método comprende además:

recibir, por la terminal, una segunda solicitud de certificación del primer elemento de red, en donde la segunda solicitud de certificación comprende el primer número aleatorio.

25 23. El método de conformidad con cualquiera de las reivindicaciones 20 a 22, caracterizado porque la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza;

una primera clave derivada, en donde la primera clave derivada se deriva de la clave

raíz utilizada para la certificación de confianza;

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

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

24. El método de conformidad con cualquiera de las reivindicaciones 19 a 23, caracterizado porque el método comprende además:

10 recibir, por la terminal, un primer resultado de certificación de confianza de la terminal desde el primer elemento de red, en donde el primer resultado de certificación de confianza se obtiene con base en la primera información de certificación y la primera información esperada.

25. El método de conformidad con la reivindicación 24, caracterizado porque la primera información esperada comprende un primer valor de verificación esperado.

15 26. El método de conformidad con la reivindicación 25, caracterizado porque la primera información esperada comprende además la primera información de certificación esperada.

27. El método de conformidad con cualquiera de las reivindicaciones 19 a 26, caracterizado porque el método comprende además:

enviar, por la terminal, la segunda información de certificación a un segundo elemento de red o a un primer nodo.

20 28. Un método de certificación, caracterizado porque el método comprende:

enviar, por un segundo elemento de red, una primera solicitud de certificación a un primer elemento de red, en donde la primera solicitud de certificación comprende información de identificación de una terminal;

25 recibir, por el primer elemento de red, la primera información de certificación de la terminal; y

obtener, por el primer elemento de red, un primer resultado de certificación de confianza de la terminal con base en la primera información de certificación y la primera información esperada.

29. El método de conformidad con la reivindicación 28, caracterizado porque la primera información de certificación comprende un primer valor de verificación, el primer valor de verificación se obtiene al procesar un primer número aleatorio e información de certificación local de la terminal por el uso de una clave simétrica, y la clave simétrica es una clave utilizada para la certificación de confianza.

30. El método de conformidad con la reivindicación 29, caracterizado porque la primera información de certificación comprende además la información de certificación local.

31. El método de conformidad con la reivindicación 29 o 30, caracterizado porque antes de recibir, por el primer elemento de red, la primera información de certificación de la terminal, el método comprende además:

enviar, por el primer elemento de red, una segunda solicitud de certificación a la terminal, en donde la segunda solicitud de certificación comprende el primer número aleatorio, y el primer número aleatorio corresponde a la información de identificación de la terminal.

32. El método de conformidad con cualquiera de las reivindicaciones 28 a 31, caracterizado porque el método comprende además el siguiente paso:

obtener, por el primer elemento de red, un primer vector de confianza que corresponde a la información de identificación de la terminal, en donde el primer vector de confianza comprende la primera información esperada.

33. El método de conformidad con la reivindicación 32, caracterizado porque el método comprende además:

enviar, por el primer elemento de red, una solicitud de vector de confianza a un tercer elemento de red, en donde la solicitud de vector de confianza comprende la información de identificación de la terminal; y

enviar, por el tercer elemento de red, el primer vector de confianza que corresponde a la información de identificación de la terminal al primer elemento de red.

34. El método de conformidad con la reivindicación 32, caracterizado porque el método comprende además:

recibir, por el primer elemento de red, el primer vector de confianza de un elemento de red de autenticación.

35. El método de conformidad con cualquiera de las reivindicaciones 29 a 34, caracterizado porque la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza;

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

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

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

10 36. El método de conformidad con cualquiera de las reivindicaciones 29 a 35, caracterizado porque el método comprende además:

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

15 37. El método de conformidad con cualquiera de las reivindicaciones 29 a 36, caracterizado porque el método comprende además:

20 enviar, por el primer elemento de red, un segundo vector de confianza al segundo elemento de red o un primer nodo, en donde el segundo vector de confianza comprende 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 comprende un segundo valor de verificación esperado.

38. El método de conformidad con la reivindicación 37, caracterizado porque el método comprende además:

25 enviar, por el tercer elemento de red, el segundo vector de confianza al primer elemento de red.

39. El método de conformidad con cualquiera de las reivindicaciones 29 a 36, caracterizado porque el método comprende además:

enviar, por el primer elemento de red, un tercer vector de confianza al segundo

elemento de red o un primer nodo, en donde el tercer vector de confianza comprende 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;

obtener, por el segundo elemento de red o el primer nodo, un segundo número aleatorio; y

obtener, por el segundo elemento de red o el primer nodo, un segundo valor de verificación esperado con base en la quinta clave derivada, el segundo número aleatorio, y la segunda información de certificación esperada.

40. El método de conformidad con la reivindicación 39, caracterizado porque el método comprende además:

enviar, por el tercer elemento de red, el tercer vector de confianza al primer elemento de red.

41. El método de conformidad con cualquiera de las reivindicaciones 37 a 40, caracterizado porque el método comprende además:

recibir, por el segundo elemento de red o el primer nodo, la segunda información de certificación de la terminal; y

obtener, por el segundo elemento de red o el primer nodo, un segundo resultado de certificación de confianza de la terminal con base en la segunda información de certificación y la segunda información esperada.

42. El método de conformidad con cualquiera de las reivindicaciones 28 a 41, caracterizado porque el método comprende además:

enviar, por el primer elemento de red, el primer resultado de certificación de confianza a la terminal.

43. Un método de certificación, caracterizado porque el método comprende:

enviar, por un segundo nodo, una tercera solicitud de certificación a un tercer nodo;

recibir, por el segundo nodo, tercera información de certificación del tercer nodo; y

obtener, por el segundo nodo, un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

5 44. El método de conformidad con la reivindicación 43, caracterizado porque la tercera información de certificación comprende 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.

45. El método de conformidad con la reivindicación 44, caracterizado porque la tercera información de certificación comprende además la información de certificación local.

10 46. El método de conformidad con cualquiera de las reivindicaciones 43 a 45, caracterizado porque la tercera información esperada comprende un tercer valor de verificación esperado.

47. El método de conformidad con la reivindicación 46, caracterizado porque la tercera información esperada comprende además la tercera información de certificación esperada.

15 48. El método de conformidad con la reivindicación 43, caracterizado porque el método comprende además:

enviar, por el segundo nodo, una solicitud de vector de confianza a un tercer elemento de red, en donde la solicitud de vector de confianza comprende información de identificación del tercer nodo; y

20 recibir, por el segundo nodo, un cuarto vector de confianza del tercer elemento de red, en donde el cuarto vector de confianza comprende la tercera información esperada.

49. El método de conformidad con cualquiera de las reivindicaciones 44 a 48, caracterizado porque la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza; y

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

50. El método de conformidad con cualquiera de las reivindicaciones 43 a 49, caracterizado porque el método comprende además:

enviar, por el segundo nodo, el resultado de certificación de confianza al tercer nodo.

51. Un método de certificación, caracterizado porque el método comprende:

recibir, por un tercer nodo, una tercera solicitud de certificación de un segundo nodo;

y

5 enviar, por el tercer nodo, la tercera información de certificación al segundo nodo, en donde la tercera información de certificación comprende 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.

10 52. El método de conformidad con la reivindicación 51, caracterizado porque la tercera información de certificación comprende además la información de certificación local.

53. El método de conformidad con la reivindicación 51 o 52, caracterizado porque la clave simétrica es cualquiera de las siguientes:

una clave raíz utilizada para la certificación de confianza; y

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

54. El método de conformidad con cualquiera de las reivindicaciones 51 a 53, caracterizado porque el método comprende además:

20 recibir, por el tercer nodo, un resultado de certificación de confianza del tercer nodo desde el segundo nodo, en donde el resultado de certificación de confianza se obtiene con base en la tercera información de certificación y la tercera información esperada.

55. El método de conformidad con la reivindicación 54, caracterizado porque la tercera información esperada comprende un tercer valor de verificación esperado.

25 56. El método de conformidad con la reivindicación 55, caracterizado porque la tercera información esperada comprende además la tercera información de certificación esperada.

57. Un método de certificación, caracterizado porque el método comprende:

enviar, por un segundo nodo, una tercera solicitud de certificación a un tercer nodo;

enviar, por el tercer nodo, la tercera información de certificación al segundo nodo; y

obtener, por el segundo nodo, un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

5 58. El método de conformidad con la reivindicación 57, caracterizado porque la tercera información de certificación comprende 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.

10 59. El método de conformidad con la reivindicación 57 o 58, caracterizado porque la tercera información esperada comprende un tercer valor de verificación esperado.

60. El método de conformidad con la reivindicación 59, caracterizado porque el método comprende además:

15 enviar, por el segundo nodo, una solicitud de vector de confianza a un tercer elemento de red, en donde la solicitud de vector de confianza comprende información de identificación del tercer nodo; y

enviar, por el tercer elemento de red, un cuarto vector de confianza al segundo nodo, en donde el cuarto vector de confianza comprende la tercera información esperada.

61. El método de conformidad con cualquiera de las reivindicaciones 58 a 60, caracterizado porque la clave simétrica es cualquiera de las siguientes:

20 una clave raíz utilizada para la certificación de confianza; y

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

62. El método de conformidad con cualquiera de las reivindicaciones 57 a 61, caracterizado porque el método comprende además:

25 recibir, por el tercer nodo, el resultado de certificación de confianza del segundo nodo.

63. Un primer elemento de red, caracterizado porque comprende: un módulo de recepción, configurado para recibir la primera información de certificación de una terminal; y

un módulo de procesamiento, configurado 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.

64. Una terminal, caracterizada porque comprende:

5 un módulo de determinación, configurado para determinar la primera información de certificación; y

un módulo de envío, configurado para enviar la primera información de certificación a un primer elemento de red.

10 65. Un sistema de comunicación, caracterizado porque el sistema comprende un primer elemento de red y un segundo elemento de red;

el segundo elemento de red se configura para enviar una primera solicitud de certificación al primer elemento de red, en donde la primera solicitud de certificación comprende información de identificación de una terminal;

15 el primer elemento de red se configura para recibir la primera información de certificación de la terminal; y

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.

66. Un segundo nodo, caracterizado porque comprende:

20 un módulo de envío, configurado para enviar una tercera solicitud de certificación a un tercer nodo;

un módulo de recepción, configurado para recibir tercera información de certificación del tercer nodo; y

25 un módulo de determinación, configurado para obtener un resultado de certificación de confianza del tercer nodo con base en la tercera información de certificación y la tercera información esperada.

67. Un tercer nodo, caracterizado porque comprende:

un módulo de recepción, configurado para recibir una tercera solicitud de certificación de un segundo nodo; y

5 un módulo de envío, configurado para enviar la tercera información de certificación al segundo nodo, en donde la tercera información de certificación comprende 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.

68. Un sistema de comunicación, caracterizado porque el sistema comprende un segundo nodo y un tercer nodo;

10 el segundo nodo se configura para enviar una tercera solicitud de certificación al tercer nodo;

el tercer nodo se configura para enviar la tercera información de certificación al segundo nodo; y

15 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.

69. Un aparato de comunicación, caracterizado porque el aparato de comunicación comprende 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
20 código de programa de computadora, el código de programa de computadora comprende instrucciones de computadora, y cuando el uno o más procesadores ejecutan las instrucciones de computadora, el aparato de comunicación se habilita para realizar el método de conformidad con cualquiera de las reivindicaciones 1 a 62.

70. Un medio de almacenamiento leíble por computadora, caracterizado porque el
25 medio de almacenamiento leíble por computadora almacena instrucciones, y cuando las instrucciones se ejecutan por un procesador, se implementa el método de conformidad con cualquiera de las reivindicaciones 1 a 62.

71. Un producto de programa de computadora, caracterizado porque comprende un programa de computadora, en donde cuando el programa de computadora se ejecuta en un
30 procesador, se implementa el método de conformidad con cualquiera de las reivindicaciones

1 a 62.