

REIVINDICACIONES

1. Un método para recibir y procesar un mensaje de datos, el método caracterizado porque comprende:

- 5 almacenar, en una memoria, una llave de cifrado;
- recibir, mediante un dispositivo de recepción, un mensaje de datos, en donde el mensaje de datos incluye un mensaje cifrado y un código de autenticación del mensaje, en donde el código de autenticación del mensaje se genera usando una parte del mensaje
- 10 cifrado antes de descifrar el mensaje cifrado;
- generar, mediante un dispositivo de procesamiento, un código de autenticación de referencia, utilizando una parte del mensaje cifrado incluido en el mensaje de datos recibido antes de descifrar el mensaje cifrado;
- 15 validar, mediante el dispositivo de procesamiento, el mensaje de datos recibido basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado; y
- 20 descifrar, mediante el dispositivo de procesamiento, el mensaje cifrado incluido en el mensaje de datos recibido, utilizando la llave de cifrado almacenada, para obtener un mensaje descifrado.

2. El método de acuerdo con la reivindicación 1,

25 caracterizado porque el mensaje de datos es un mensaje del servicio

de notificación a distancia recibido por medio de un servicio de notificación a distancia.

3. El método de acuerdo con la reivindicación 1,
5 caracterizado porque:

la memoria está además configurada para almacenar un contador de referencia, y

la validación del mensaje de datos recibido incluye además comprobar el contador de mensajes incluido en el mensaje
10 de datos recibido contra el contador de referencia almacenado.

4. El método de acuerdo con la reivindicación 1, caracterizado porque comprende además:

transmitir, mediante un dispositivo de transmisión, una
15 notificación de recepción en respuesta al mensaje de datos recibido.

5. El método de acuerdo con la reivindicación 4, caracterizado porque comprende además:

realizar, mediante el dispositivo de procesamiento, una
20 acción basándose en el mensaje descifrado;

generar, mediante el dispositivo de procesamiento, un mensaje de regreso como resultado de, o basándose en la acción realizada;

cifrar, mediante el dispositivo de procesamiento, el
25 mensaje de regreso generado, utilizando la llave de cifrado

almacenada, para obtener un mensaje de regreso cifrado; y

generar, mediante el dispositivo de procesamiento, un código de autenticación de regreso, utilizando una parte del mensaje de regreso cifrado, en donde:

5 la notificación de recepción transmitida incluye el mensaje de regreso cifrado y el código de autenticación de regreso.

6. El método de acuerdo con la reivindicación 5, caracterizado porque:

10 la memoria incluye además un contador de regreso, y
 la notificación de recepción transmitida incluye, además, el contador de regreso.

7. El método de acuerdo con la reivindicación 1, caracterizado porque:

15 la memoria incluye, además, una regla de generación de códigos de autenticación, y
 el código de autenticación de referencia se genera basándose en la aplicación de la regla de generación de código de autenticación almacenada, para la parte del mensaje cifrado
20 incluida en el mensaje de datos recibido.

8. El método de acuerdo con la reivindicación 1, caracterizado porque comprende además:

25 agregar un esquema de relleno, mediante el dispositivo

de procesamiento, al mensaje cifrado incluido en el mensaje del servicio de notificación a distancia recibido utilizando una llave del esquema de relleno, en donde:

la parte del mensaje cifrado utilizada para generar el
5 código de autenticación de referencia es el mensaje cifrado con esquema de relleno.

9. El método de acuerdo con la reivindicación 8, caracterizado porque la llave de relleno es la llave de cifrado.

10

10. El método de acuerdo con la reivindicación 1, caracterizado porque comprende además:

comprobar, mediante el dispositivo de procesamiento, un formato de datos del mensaje descifrado basándose en una regla de
15 formateo de datos.

11. El método de acuerdo con la reivindicación 1, caracterizado porque el mensaje descifrado incluye uno de: un perfil de tarjeta digitalizada y una llave de un solo uso para utilizarse en
20 una transacción de pago.

12. El método de acuerdo con la reivindicación 1, caracterizado porque el código de autenticación de referencia se genera adicionalmente utilizando la llave de cifrado almacenada.

25

13. El método de acuerdo con la reivindicación 1, caracterizado porque la memoria es una memoria de elemento no seguro de un dispositivo de comunicación móvil.

5 14. Un sistema para llevar a cabo el método de la reivindicación 1, el sistema caracterizado porque comprende:

 una memoria configurada para almacenar una llave de cifrado;

 un dispositivo de recepción configurado para recibir un
10 mensaje de datos, en donde el mensaje de datos incluye un mensaje cifrado y un código de autenticación del mensaje, en donde el código de autenticación del mensaje se genera utilizando una parte del mensaje cifrado antes de descifrar el mensaje cifrado; y

 un dispositivo de procesamiento configurado para:
15 generar un código de autenticación de referencia utilizando una parte del mensaje cifrado incluido en el mensaje de datos recibido antes de descifrar el mensaje cifrado,

 validar los datos recibidos basándose en una comprobación del código de autenticación del mensaje incluido en
20 el mensaje de datos recibido contra el código de autenticación de referencia generado, y

 descifrar el mensaje cifrado incluido en el mensaje de datos recibido utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.

15. El sistema de acuerdo con la reivindicación 14, caracterizado porque el mensaje de datos es un mensaje del servicio de notificación a distancia recibido por medio de un servicio de notificación a distancia.

5

16. El sistema de acuerdo con la reivindicación 14, caracterizado porque:

la memoria está además configurada para almacenar un contador de referencia, y

10 la validación del mensaje de datos recibido incluye además comprobar el contador de mensajes incluido en el mensaje de datos recibido contra el contador de referencia almacenado.

15 17. El sistema de acuerdo con la reivindicación 14, caracterizado porque comprende además:

un dispositivo de transmisión configurado para transmitir una notificación de recepción en respuesta al mensaje del servicio de notificación a distancia recibido.

20 18. El sistema de acuerdo con la reivindicación 17, caracterizado porque:

el dispositivo de procesamiento está configurado además para:

25 realizar una acción basándose en el mensaje descifrado,

generar un mensaje de regreso como resultado de,
o basándose en la acción realizada,

cifrar el mensaje de regreso generado utilizando la
llave de cifrado almacenada para obtener un mensaje de regreso
5 cifrado, y

generar un código de autenticación de regreso
utilizando una parte del mensaje de regreso cifrado, y

la notificación de recepción transmitida incluye el
mensaje de regreso cifrado, el contador de regreso, y el código de
10 autenticación de regreso.

19. El sistema de acuerdo con la reivindicación 18,
caracterizado porque:

la memoria incluye además un contador de regreso, y
15 la notificación de recepción transmitida incluye, además,
el contador de regreso.

20. El sistema de acuerdo con la reivindicación 14,
caracterizado porque:

20 la memoria incluye, además, una regla de generación de
códigos de autenticación, y

el código de autenticación de referencia se genera
basándose en la aplicación de la regla de generación de código de
autenticación almacenadas, a la parte del mensaje cifrado incluida
25 en el mensaje del servicio de notificación a distancia recibido.

21. El sistema de acuerdo con la reivindicación 14, caracterizado porque:

5 el dispositivo de procesamiento está configurado, además, para agregar un esquema de relleno al mensaje cifrado incluido en el mensaje del servicio de notificación a distancia recibido, utilizando una llave de esquema de relleno, y

10 la parte del mensaje cifrado usada para generar el código de autenticación de referencia es el mensaje cifrado con el esquema de relleno.

22. El sistema de acuerdo con la reivindicación 21, caracterizado porque la llave del esquema de relleno es la llave de cifrado.

15

23. El sistema de acuerdo con la reivindicación 14, caracterizado porque el dispositivo de procesamiento está configurado, además, para comprobar un formato de datos del mensaje descifrado basándose en una regla de formateo de datos.

20

24. El sistema de acuerdo con la reivindicación 14, caracterizado porque el mensaje descifrado incluye uno de: un perfil de tarjeta digitalizada y una llave de un solo uso para utilizarse en una transacción de pago.

25

25. El sistema de acuerdo con la reivindicación 14, caracterizado porque el código de autenticación de referencia se genera adicionalmente utilizando la llave de cifrado almacenada.

5 26. El sistema de acuerdo con la reivindicación 14, caracterizado porque la memoria es una memoria de elemento no seguro de un dispositivo de comunicación móvil.

10

15

20

25