

REIVINDICACIONES

1. Un método para generar credenciales de pago en una transacción de pago, el cual está caracterizado porque comprende:

almacenar, en una memoria, una llave de un solo uso asociada con una cuenta de transacciones;

recibir, mediante un dispositivo de recepción, un número de identificación personal;

identificar, mediante un dispositivo de procesamiento, una primera llave de sesión;

generar, mediante el dispositivo de procesamiento, una llave segunda sesión basándose en la llave de un solo uso almacenada y el número de identificación personal recibido;

15 generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en la primera llave de sesión;

generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en la segunda llave de sesión; y

20 transmitir, mediante un dispositivo de transmisión, el primer criptograma de la aplicación y el segundo criptograma de la aplicación.

2. El método de acuerdo con la reivindicación 1, el cual comprende además:

25 almacenar, en la memoria, una llave maestra de la tarjeta

asociada con la cuenta de transacciones, en donde:

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión basándose en la llave maestra de la tarjeta almacenada.

3. El método de acuerdo con la reivindicación 1, el cual comprende además:

almacenar, en la memoria, un contador de transacciones de la aplicación, en donde:

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión basándose en el contador de transacciones de la aplicación almacenado.

4. El método de acuerdo con la reivindicación 1, el cual comprende además:

validar, mediante el dispositivo de procesamiento, el número de identificación personal recibido antes de generar la segunda llave de sesión.

5. El método de acuerdo con la reivindicación 4, en donde el dispositivo de procesamiento está configurado para generar una segunda llave de sesión inválida si falla la validación del número de identificación personal recibido.

6. El método de acuerdo con la reivindicación 1, en donde el primer criptograma de la aplicación y el segundo criptograma de la aplicación se transmiten hasta un dispositivo de punto de venta.

7. El método de acuerdo con la reivindicación 1, en donde la memoria es una memoria de elemento no seguro de un dispositivo de comunicación móvil.

8. Un método para generar credenciales de pago en una transacción de pago, el cual comprende:

almacenar, en una memoria, una llave maestra de la tarjeta asociada con una cuenta de transacciones;

generar, mediante un dispositivo de procesamiento, una primera llave de sesión basándose en la llave maestra de la tarjeta almacenada;

generar, mediante el dispositivo de procesamiento, una segunda llave de sesión;

generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en la primera llave de sesión;

generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en la segunda llave de sesión; y

transmitir, mediante un dispositivo de transmisión, el primer criptograma de la aplicación y el segundo criptograma de la aplicación.

9. El método de acuerdo con la reivindicación 8, el cual comprende además:

almacenar, en la memoria, un número de secuencia de la cuenta de transacciones asociado con la cuenta de transacciones, en

donde:

la primera llave de sesión se basa además en el número de secuencia de la cuenta transacciones almacenada.

10. El método de acuerdo con la reivindicación 8, el cual
5 comprende además:

almacenar, en la memoria, una llave maestra de la segunda tarjeta asociada con la cuenta de transacciones, en donde:

la segunda llave de sesión se basa en la llave maestra de la segunda tarjeta almacenada.

10 11. El método de acuerdo con la reivindicación 8, el cual comprende además:

recibir, mediante un dispositivo de recepción, un primer criptograma de la aplicación correspondiente y un segundo criptograma de la aplicación correspondiente;

15 validar, mediante el dispositivo de procesamiento, (i) el primer criptograma de la aplicación correspondiente recibido, basado en el primer criptograma de la aplicación generado, y (ii) el segundo criptograma de la aplicación correspondiente recibido, basado en el segundo criptograma de la aplicación generado; y

20 transmitir, mediante el dispositivo de transmisión, un resultado de la validación.

12. El método de acuerdo con la reivindicación 11, en donde el primer criptograma de la aplicación correspondiente y el segundo criptograma de la aplicación correspondiente se reciben desde un
25 dispositivo de punto de venta.

13. El método de acuerdo con la reivindicación 11, en donde el resultado de la validación se transmite a una institución financiera asociada con la cuenta de transacciones.

14. Un sistema para generar credenciales de pago en una transacción de pago mediante el método de la reivindicación 1, el cual está caracterizado porque comprende:

una memoria configurada para almacenar una llave de un solo uso asociada con una cuenta de transacciones;

un dispositivo de recepción configurado para recibir un número de identificación personal;

un dispositivo de procesamiento configurado para:

identificar una primera llave de sesión,

generar una segunda llave de sesión basándose en la llave de un solo uso almacenada y el número de identificación personal recibido,

generar un primer criptograma de la aplicación basándose en la primera llave de sesión, y

generar un segundo criptograma de la aplicación basándose en la segunda llave de sesión; y

un dispositivo de transmisión configurado para transmitir el primer criptograma de la aplicación y el segundo criptograma de la aplicación.

15. El sistema de acuerdo con la reivindicación 14, en donde:

la memoria está configurada además para almacenar una llave maestra de la tarjeta asociada con la cuenta de transacciones,

y

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión basándose en la llave maestra de la tarjeta almacenada.

16. El sistema de acuerdo con la reivindicación 14, en donde:
la memoria está configurada además para almacenar un contador de transacciones de la aplicación, y
la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión, basándose en el contador de transacciones de la aplicación almacenado.

17. El sistema de acuerdo con la reivindicación 14, en donde el dispositivo de procesamiento está configurado además para validar el número de identificación personal recibido antes de generar la segunda llave de sesión.

18. El sistema de acuerdo con la reivindicación 17, en donde el dispositivo de procesamiento está configurado para generar una segunda llave de sesión inválida si falla la validación del número de identificación personal recibido.

19. El sistema de acuerdo con la reivindicación 14, en donde el primer criptograma de la aplicación y el segundo criptograma de la aplicación se transmiten hasta un dispositivo de punto de venta.

20. El sistema de acuerdo con la reivindicación 14, en donde la memoria es una memoria de elemento no seguro de un dispositivo

de comunicación móvil.

21. Un sistema para generar credenciales de pago en una transacción de pago, el cual comprende:

una memoria configurada para almacenar una llave
5 maestra de la tarjeta asociada con una cuenta de transacciones;

un dispositivo de procesamiento configurado para:

generar una primera llave de sesión basándose en
la llave maestra de la tarjeta almacenada,

generar una segunda llave de sesión,

10 generar un primer criptograma de la aplicación
basándose en la primera llave de sesión, y

generar un segundo criptograma de la aplicación
basándose en la segunda llave de sesión; y

un dispositivo de transmisión configurado para transmitir
15 el primer criptograma de la aplicación y un segundo criptograma de
la aplicación.

22. El sistema de acuerdo con la reivindicación 21, en donde:

la memoria está configurada además para almacenar un
número de secuencia de cuenta de transacciones asociado con la
20 cuenta de transacciones, y

la primera llave de sesión se basa además en el número
de secuencia de la cuenta de transacciones almacenado.

23. El sistema de acuerdo con la reivindicación 21, en donde:

la memoria está además configurada para almacenar una
25 llave maestra de la segunda tarjeta asociada con la cuenta de

transacciones, y

la segunda llave de sesión se basa en la llave maestra de la segunda tarjeta almacenada.

24. El sistema de acuerdo con la reivindicación 21, el cual
5 comprende, además:

un dispositivo de recepción configurado para recibir un primer criptograma de la aplicación correspondiente y un segundo criptograma de la aplicación correspondiente, en donde:

el dispositivo de procesamiento está configurado además
10 para validar (i) el primer criptograma de la aplicación correspondiente recibido basado en el primer criptograma de la aplicación generado, y (ii) el segundo criptograma de la aplicación correspondiente recibido basado en el segundo criptograma de la aplicación generado, y

15 el dispositivo de transmisión está configurado además para transmitir un resultado de la validación.

25. El sistema de acuerdo con la reivindicación 24, en donde el dispositivo de recepción está configurado además para recibir el primer criptograma de la aplicación correspondiente y el segundo
20 criptograma de la aplicación correspondiente desde un dispositivo de punto de venta.

26. El sistema de acuerdo con la reivindicación 24, en donde el dispositivo de transmisión está configurado además para transmitir el resultado de la validación a una institución financiera asociada con
25 la cuenta de transacciones.