

REIVINDICACIONES

1. Un método para construir una llave de almacenamiento avanzada que comprende:

almacenar, en una memoria de un dispositivo de comunicación móvil,

información de dispositivo asociada con el dispositivo de comunicación móvil,

código de programa asociado con un primer programa de aplicación, en donde el código de programa incluye un identificador de instancia, y

código de programa asociado con un segundo programa de aplicación, en donde el código de programa incluye una primera llave;

15 generar, mediante un dispositivo de procesamiento, una huella de dispositivo asociada con el dispositivo de comunicación móvil con base en la información de dispositivo almacenada vía la ejecución del código de programa asociado con el primer programa de aplicación;

20 generar, mediante el dispositivo de procesamiento, un valor aleatorio vía ejecución del código de programa asociado con el primer programa de aplicación;

 construir, mediante el dispositivo de procesamiento, un valor diversificador con base en la huella de dispositivo generada, el valor
25 aleatorio generado y el identificador de instancia incluido en el

código de programa asociado con el primer programa de aplicación;
y

descifrar, mediante el dispositivo de procesamiento, el valor
diversificador construido con la primera llave almacenada en el
5 código de programa asociado con el segundo programa de aplicación
vía la ejecución del código de programa asociado con el segundo
programa de aplicación para obtener una llave de almacenamiento.

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

10 almacenar, en una base de datos local del dispositivo de
comunicación móvil, datos protegidos; y

cifrar, mediante el dispositivo de procesamiento, los datos
protegidos almacenados en la base de datos local con la llave de
almacenamiento.

15 3. El método de acuerdo con la reivindicación 1, en donde la
información de dispositivo incluye uno o más identificadores únicos
asociados con el dispositivo de comunicación móvil.

4. El método de acuerdo con la reivindicación 1, en donde el
valor aleatorio es un número aleatorio o pseudoaleatorio.

20 5. El método de acuerdo con la reivindicación 1, en donde el
identificador de instancia es único para una instancia del primer
programa de aplicación.

6. El método de acuerdo con la reivindicación 1, en donde el
segundo programa de aplicación es configurado para realizar la
25 criptografía de *white-box* con la primera llave.

7. El método de acuerdo con la reivindicación 1, en donde la primera llave es una llave dinámica.

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

5 almacenar, en la memoria, datos de programa asociados con el primer programa de aplicación; y

 almacenar, en los datos de programa asociados con el primer programa de aplicación, el valor aleatorio generado.

9. El método de acuerdo con la reivindicación 1, en donde el
10 código de programa asociado con el segundo programa de aplicación es incluido en el código de programa asociado con el primer programa de aplicación.

10. El método de acuerdo con la reivindicación 9, en donde el
segundo programa de aplicación es una función ejecutable del primer
15 programa de aplicación.

11. El método de acuerdo con la reivindicación 1, que comprende además:

 transmitir, mediante un dispositivo de transmisión, el valor aleatorio generado;

20 recibir, mediante un dispositivo de recepción, uno o más parámetros cifrados, en donde el uno o más parámetros cifrados son cifrados cada uno con la llave de almacenamiento; y

 almacenar, en una base de datos local del dispositivo de comunicación móvil, el uno o más parámetros cifrados recibidos.

25 12. El método de acuerdo con la reivindicación 11, en donde

transmitir el valor aleatorio generado incluye además transmitir el identificador de instancia.

13. Un sistema para construir una llave de almacenamiento avanzada, que comprende:

5 una memoria de un dispositivo de comunicación móvil configurada para almacenar

información de dispositivo asociada con el dispositivo de comunicación móvil,

código de programa asociado con un primer programa de aplicación, en donde el código de programa incluye un identificador de instancia, y

código de programa asociado con un segundo programa de aplicación, en donde el código de programa incluye una primera llave; y

15 un dispositivo de procesamiento configurado para

generar una huella de dispositivo asociada con el dispositivo de comunicación móvil con base en la información de dispositivo almacenada vía ejecución del código de programa asociado con el primer programa de aplicación,

20 generar un valor aleatorio vía ejecución del código de programa asociado con el primer programa de aplicación,

construir un valor diversificador con base en la huella de dispositivo generada, el valor aleatorio generado y el identificador de instancia incluido en el código de programa asociado con el primer

25 programa de aplicación y

descifrar el valor diversificador construido con la primera llave almacenada en el código de programa asociado con el segundo programa de aplicación vía ejecución del código de programa asociado con el segundo programa de aplicación para obtener una
5 llave de almacenamiento.

14. El sistema de acuerdo con la reivindicación 13, que comprende además:

una base de datos local del dispositivo de comunicación móvil configurada para almacenar datos protegidos, en donde
10 el dispositivo de procesamiento es configurado adicionalmente para cifrar los datos protegidos almacenados en la base de datos local con la llave de almacenamiento.

15 15. El sistema de acuerdo con la reivindicación 13, en donde la información de dispositivo incluye uno o más identificadores únicos asociados con el dispositivo de comunicación móvil.

16. El sistema de acuerdo con la reivindicación 13, en donde el valor aleatorio es un número aleatorio o pseudoaleatorio.

20 17. El sistema de acuerdo con la reivindicación 13, en donde el identificador de instancia es único para una instancia del primer programa de aplicación.

18. El sistema de acuerdo con la reivindicación 13, en donde el segundo programa de aplicación es configurado para realizar criptografía de *white-box* con la primera llave.

25 19. El sistema de acuerdo con la reivindicación 13, en donde la primera llave es una llave dinámica.

20. El sistema de acuerdo con la reivindicación 13, en donde la memoria es configurada adicionalmente para almacenar datos de programa asociados con el primer programa de aplicación, y

5 el dispositivo de procesamiento es configurado adicionalmente para almacenar, en los datos de programa asociados con el primer programa de aplicación, el valor aleatorio generado.

21. El sistema de acuerdo con la reivindicación 13, en donde el código de programa asociado con el segundo programa de aplicación es incluido en el código de programa asociado con el primer programa de aplicación.

22. El sistema de acuerdo con la reivindicación 21, en donde el segundo programa de aplicación es una función ejecutable del primer programa de aplicación.

15 23. El sistema de acuerdo con la reivindicación 13, que comprende además:

un dispositivo de transmisión configurado para transmitir el valor aleatorio generado; y

20 un dispositivo de recepción configurado para recibir uno o más parámetros cifrados, en donde el uno o más parámetros cifrados son cifrados cada uno con la llave de almacenamiento, en donde

el dispositivo de procesamiento es configurado adicionalmente para almacenar, en una base de datos local del dispositivo de comunicación móvil, el uno o más parámetros cifrados.

25 24. El sistema de acuerdo con la reivindicación 23, en donde la

transmisión de valor aleatorio generado incluye además transmitir el identificador de instancia.

5

10

15

20

25