

REIVINDICACIONES

1. Un método para actualizar transaccionalmente la información en un chip de un dispositivo móvil usando un servidor de una red operacional que comprende:

recibir una solicitud por un usuario a través de una aplicación que corre en un dispositivo móvil para una operación transaccional;

leer la información de un chip en respuesta a la solicitud de la aplicación móvil;

encriptar la información transaccional leída del chip;

transferir la información transaccional encriptada remotamente al servidor de la red operacional;

realizar una autenticación en el servidor de la red operacional;

realizar una autenticación con una primera llave de emisor; y

actualizar la información en el chip basado en una respuesta transaccional del servidor de la red operacional;

encriptar, mediante una segunda llave, las llaves de lectura y escritura asociadas con un número de serie del chip

en donde la aplicación móvil se compone de un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.

2. El método de acuerdo con la reivindicación 1, que comprende además utilizar múltiples llaves criptográficas juntas a lo largo de los pasos de autenticación.

3. El método de acuerdo con la reivindicación 1, que comprende además asegurar la integridad de la información

transaccional transferida remotamente con un modelo criptográfico, reduciendo la posibilidad de fraude.

4. El método de acuerdo con la reivindicación 3, en donde el modelo criptográfico reduce la posibilidad de fraude por inserción de un agente fraudulento entre la aplicación móvil y el servidor de la red operacional.

5. El método de acuerdo con la reivindicación 1, en donde la información transaccional es transferida e interpretada por el servidor de la red operacional utilizando una segunda llave; y
en donde el número de serie es proporcionado por un agente de envío.

6. Un método para actualizar transicionalmente actualizar la información en un chip de un dispositivo móvil utilizando un servidor de una red operacional que comprende:

recibir una solicitud por un usuario a través de una aplicación móvil que corre en un dispositivo móvil para una operación transaccional;

leer información del chip en respuesta a la solicitud de la aplicación móvil;

generar una primera llave encriptada para asegurar la integridad de la información transaccional leída del chip;

encriptar la información transaccional para transferencia remota;

transferir la información transaccional encriptada remotamente al servidor de la red operacional;

devolver una respuesta transaccional a la aplicación móvil que corre en el dispositivo móvil por el servidor de la red operacional; y

actualizar la información en el chip en base a la respuesta transaccional del servidor en la red operacional;

utilizar una segunda llave encriptada enlazada a la transacción para encriptar las llaves de lectura y escritura asociadas con el número de serie del chip y proporcionada por el agente emisor;

en donde la aplicación móvil comprende un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.

7. El método de la reivindicación 6 que comprende, además, por parte del servidor en la red operacional:

probar la integridad de la información transaccional;

realizar una autenticación con una llave de emisor de un agente emisor;

y

determinar la respuesta transaccional.

8. El método de la reivindicación 6, en donde la prueba de integridad para la información transaccional comprende usar un modelo criptográfico, reduciendo la posibilidad de fraude por inserción de un agente fraudulento entre la aplicación móvil y el servidor de la red operacional.