

REIVINDICACIONES

1. Método con el fin de promover la lectura o grabación en chips utilizados entre diversos fines como medio de pago a través de dispositivos móviles tales como teléfonos inteligentes, tabletas, notebooks, relojes inteligentes, el método permite un proceso transaccional de actualización y autenticación de información entre un chip de tipo sin contacto y un servidor de red operativo y se realiza utilizando un sistema móvil para la actualización transaccional de información, el sistema móvil comprende el chip tipo sin contacto y el servidor de red operativo y un dispositivo móvil, en donde el método comprende tres pasos marco de un proceso transaccional de actualización y información de autenticación entre el chip de tipo sin contacto y el servidor de red operativo, en el que los tres pasos marco comprenden:

En un primer paso marco, una solicitud de usuario a través de una aplicación móvil donde:

- Aproximar el chip y al dispositivo móvil; y
- solicitud por parte de un usuario a través de la aplicación móvil para consulta o registro de información;
- leer la información en ese chip por la aplicación móvil y luego procesar y cifrar la transacción solicitada por el usuario a través de una primera clave generada para garantizar la integridad de la información transaccional para la transferencia remota;

En un segundo paso macro una autenticación en el Servidor de Red Operacional combinado con un tercer paso macro de autenticación con la clave del Emisor, comprendiendo el segundo y tercer paso;

-transferir e interpretar por el servidor de la red operativa la información transaccional,

- el servidor operativo realiza pruebas de integridad para la información transaccional y usa una segunda clave que encripta las claves de lectura/escritura del chip propiedad de un agente de envío respectivo, y
- la segunda clave está vinculada a la respectiva transacción de solicitud de autorización de recarga;
- realizar una autenticación con una clave de emisor que es una tercera clave de un agente emisor, la tercera clave cifrada vinculada a la transacción para cifrar claves de lectura y escritura asociadas con un número de serie de chip del chip y proporcionada por el agente emisor;
- luego devolver, por parte del servidor, la respuesta transaccional a la aplicación móvil ejecutada por el dispositivo móvil del usuario; y actualizar la información en el chip, completando la operación transaccional.

2. Método según la reivindicación 1, donde la aplicación móvil está protegida por una capa de seguridad para evitar su lectura por parte de técnicos no autorizados o posibles estafadores.

3. Método según la reivindicación 1, que comprende un modelo criptográfico para asegurar la integridad de la información transaccional transferida remotamente, reduciendo la posibilidad de fraude por inserción de un agente fraudulento entre la aplicación cliente y el servidor de comunicaciones de la red operativa.