CLAIMS

1. A method for securing updating transaction messages transiting between a mobile application in a mobile device and an update issuer through a gateway wherein when an update transaction of the mobile is initiated,

(a) the mobile application being operated to perform the following steps:

- incrementing a transaction counter,

- deriving a session encryption key ENC from the transaction counter value and a gateway encryption key KENC, said gateway encryption key being derived from a first master gateway key,

- encrypting sensitive data with the session encryption key ENC,

- deriving a session integrity key MAC from the transaction counter value and a gateway integrity key KMAC, said gateway integrity key being derived from a second master gateway key,

- computing a MAC signature value from the session integrity key MAC and at least one part of the contents of the transaction request message,

- elaborating an update transaction request message comprising the encrypted sensitive data, the transaction counter value, the MAC signature value, and an application identifier of the mobile application,

- sending the transaction request message from the mobile application through the mobile device to the gateway,

(b) the gateway being configured to perform the following steps:

authenticating the upgrade transaction request message by the gateway comprises the following steps:

- computing the session encryption key from the received transaction request message, and

- decrypting the received encrypted data with the computed session encryption key ENC,

-computing the session integrity key from the received transaction request message, and

- verifying the MAC signature value of the received transaction request message,

- decrypting the sensitive data of the update transaction request message,

- sending the update transaction request message comprising the decrypted sensitive data to the update issuer of the mobile application for processing, and

- forwarding an update response message from the issuer to the mobile application for configuration of the mobile application.

2. The method according to claim 1, wherein the loading of the gateway encryption key KENC and the gateway integrity key KMAC into the mobile application comprises the following steps:

- generation of the first and second master gateway keys,

- generation of the application identifier for the mobile application,

- deriving the gateway encryption key KENC from said application identifier, the first master key and a first derivation algorithm,

- deriving the gateway integrity key KMAC from said application identifier, the second master key and a second derivation algorithm,

- loading into the mobile application the generated application identifier, the derived gateway encryption key KENC and the derived gateway integrity key KMAC.

3. The method according to any one of claims 1 to 2, wherein the gateway computes the session keys according to the following steps:

- deriving the gateway encryption key KENC and the gateway integrity key KMAC from the received application identifier and respectively from a stored first and second master gateway key and the first and second derivation algorithm,

- deriving the session encryption key ENC and the session integrity key MAC from the received transaction counter value and respectively from the derived gateway encryption key KENC and the derived gateway integrity key KMAC.

4. The method according to claim 2 or claim 3, wherein the first and the second derivation algorithm are identical.

5. The method according to any one of claims 2 to 4, wherein the first and the second master gateway key are identical.

6. The method according to any one of claims 1 to 5, wherein the mobile application comprising the generated application identifier, the gateway encryption key KENC and the gateway integrity key KMAC are stored into a secure element of the mobile device.

7. The method according to any one of the preceding claims, wherein the update transaction is initiated by a user of the mobile device, by the mobile device itself, or when a push message is received by the mobile application.

8. The method according to any one of the preceding claims, wherein the mobile application is a mobile payment application, the transaction counter is an Application Transaction Counter (ATC) and wherein the update transaction request message comprises:

- the application identifier,
- the current Application Transaction Counter ATC,
- the sensitive data comprising the contents of the magnetic-stripe data track(s), fully or partially (track 1, track 2, track 3),
- dynamic transaction data and static application data enabling the issuer to authenticate the mobile payment application.

9. The method according to claim 8, wherein the update transaction initiated is an over-the-air issuer update comprising:

- updating parameters for the mobile payment application,
- blocking a payment application on the mobile device,
- unblocking the mobile payment application,
- unblocking a PIN on the mobile payment application, and/or
- changing the PIN on the mobile payment application.

10. The method according to any one of claims 1 to 8, wherein the update transaction request initiated is an authentication of the mobile device by the issuer.

11. The method according to any one of claims 1 to 8, wherein the update transaction request initiated is a payment transaction through the mobile device.

12. The method according to any one of the preceding claims, wherein the gateway communicates with the issuer through a secured processing network.

13. An update transaction processing system, comprising a mobile application stored into a mobile device, said mobile application being configured to communicate with an issuer via the mobile device across a gateway, wherein update transaction messages transiting between the mobile application and the gateway during this communication are secured according to any one of the preceding claims.