CLAIMS

1. A method of processing a remote transaction initiated by a mobile device, the method comprising:

receiving, by a server computer, a payment request including encrypted payment information and a transaction processor certificate, the encrypted payment information being generated by a mobile payment application of the mobile device, wherein the encrypted payment information is encrypted using a third party key;

decrypting, by the server computer, the encrypted payment information using the third party key;

determining, by the server computer, a transaction processor public key associated with the payment information, wherein determining the transaction processor public key further comprises:

validating that the transaction processor certificate is authentic;

verifying that the transaction processor certificate is currently valid with a certificate authority; and

extracting the transaction processor public key from the transaction processor certificate;

re-encrypting, by the server computer, the payment information using the transaction processor public key; and

sending, by the server computer, a payment response including the re-encrypted payment information to a transaction processor, wherein the transaction processor decrypts the re-encrypted payment information using a transaction processor private key and initiates a payment transaction using the decrypted payment information.

2. The method of claim 1, wherein the encrypted payment information includes encrypted payment credentials and unencrypted transaction information.

3. The method of claim 2, wherein the payment credentials are stored in a secure memory of the mobile device and the mobile payment application obtains the payment credentials from the secure memory.

4. The method of claim 3, wherein the payment credentials include an account identifier and an expiration date.

5. The method of claim 4, wherein the payment credentials further include a dynamic value generated using a shared algorithm associated with a payment processing network.

6. The method of claim 1, wherein the transaction processor initiates the payment transaction by mapping the decrypted payment information to an authorization request message configured to be processed by a payment processing network.

7. The method of claim 1, wherein the transaction processor is a merchant server computer, the transaction processor public key is a merchant public key, and the transaction processor private key is a merchant private key.

8. The method of claim 1, wherein the transaction processor is a merchant application on the mobile device, the transaction processor public key is a merchant application public key, and the transaction processor private key is a merchant application private key.

9. The method of claim 8, wherein the merchant application of the mobile device initiates the payment transaction by sending the decrypted payment information to a merchant server computer and wherein the merchant server computer generates an authorization request message for the payment transaction using the decrypted payment information.

10. The method of claim 1, wherein the transaction processor is an acquirer computer, the transaction processor public key is an acquirer public key, and the transaction processor private key is an acquirer private key.

11. The method of claim 1, wherein the third party key includes a third party public/private key pair including a third party public key and a third party private key, wherein the encrypted payment information is encrypted using the third party public key, and wherein the encrypted payment information is decrypted using the third party private key.

12. The method of claim 11, wherein the server computer, the third party public key, and the third party private key are associated with a mobile wallet provider.

13. The method of claim 11, wherein the server computer, the third party public key, and the third party private key are associated with a payment processing network.

14. The method of claim 11, wherein the payment request further comprises the third party public key and a message authentication code, and wherein decrypting the encrypted payment information further comprises:

determining, by the server computer, an account identifier using the encrypted payment information, the message authentication code, the third party public key, the third party private key associated with the server computer, a shared key derivation function with the mobile payment application, and a shared message authentication function with the mobile payment application, wherein the encrypted payment information was generated by the mobile payment application using the account identifier.

15. A server computer comprising:

a processor; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code, executable by the processor, for performing a method of processing a remote transaction, the method comprising:

receiving a payment request including encrypted payment information and a transaction processor certificate, the encrypted payment information being generated by a mobile payment application of a mobile device, wherein the encrypted payment information is encrypted using a third party key;

decrypting the encrypted payment information using a third party key;

determining a transaction processor public key associated with the payment information, wherein determining the transaction processor public key further comprises:

validating that the transaction processor certificate is authentic;

verifying that the transaction processor certificate is currently valid with a certificate authority; and

extracting the transaction processor public key from the transaction processor certificate;

re-encrypting the payment information using the transaction processor public key; and

sending a payment response including the re-encrypted payment information to a transaction processor, wherein the transaction processor decrypts the re-encrypted payment information using a transaction processor private key and initiates a payment transaction using the decrypted payment information.

16. The server computer of claim 15, wherein the encrypted payment information includes encrypted payment credentials, and wherein the payment credentials are stored in a secure memory of the mobile device and the mobile payment application obtains the payment credentials from the secure memory.

17. The server computer of claim 16, wherein the payment credentials include an account identifier and an expiration date.

18. The server computer of claim 17, wherein the payment credentials further include a dynamic value generated using a shared algorithm associated with a payment processing network.

19. The server computer of claim 15, wherein the transaction processor initiates the payment transaction by mapping the decrypted payment information to an authorization request message configured to be processed by a payment processing network.

20. The server computer of claim 15, wherein the transaction processor is a merchant server computer, the transaction processor public key is a merchant public key, and the transaction processor private key is a merchant private key.

21. The server computer of claim 15, wherein the transaction processor is a merchant application on the mobile device, the transaction processor public key is a merchant application public key, and the transaction processor private key is a merchant application private key.

22. The server computer of claim 21, wherein the merchant application on the mobile device initiates the payment transaction by sending the decrypted payment information to a merchant server computer and wherein the merchant server computer generates an authorization request message for the payment transaction.