CLAIMS

1. A method for a mobile payment, the method comprising:

receiving device authorization function enabling request information sent by a second mobile device, wherein the device authorization function enabling request information comprises a device certificate of the second mobile device;

verifying, whether the device certificate is valid;

sending verification method information to the second mobile device if the device certificate is valid, so that the second mobile device obtains verification data based on the verification method information;

receiving the verification data sent by the second mobile device;

detecting, whether the verification data is correct;

enabling a device authorization function of the second mobile device if the verification data is correct;

sending enabling information of the second mobile device to the second mobile device, so that the second mobile device confirms the enabling information;

receiving first mobile device identity authentication information sent by the second mobile device, wherein the first mobile device identity authentication information comprises first mobile device identifier information uniquely identifying a first mobile device and comprising a unique hardware code of the first mobile device or a certificate of the first mobile device;

receiving payment information sent by the second mobile device, wherein:

the payment information comprises the first mobile device identifier information, an account corresponding to a payment APP currently running in the second mobile device, and a payment amount corresponding to the first mobile device identifier information,

the first mobile device identifier information is sent by the first mobile device to the second mobile device, and

no payment APP is installed in the first mobile device, a payment APP being an APP configured to provide payment request information to a financial server configured to perform a corresponding operation on a user account included in the payment request information;

obtaining account information corresponding to the first mobile device identifier information;

and

transferring the payment amount from the account corresponding to the first mobile device identifier information to the account corresponding to the payment APP currently running in the second mobile device.

2. The method according to claim 1, wherein the first mobile device and/or the second mobile device are devices authenticated by the Internet Finance Authentication Alliance (IFAA) or an authority by using a public key infrastructure (PKI) system.

3. The method according to any one of claims 1 or 2, wherein after it is verified that the device certificate is valid, the method further comprises the following:

obtaining account credit information corresponding to the second mobile device, wherein the credit information is used to evaluate credit of the second mobile device;

detecting whether the account credit information corresponding to the second mobile device exceeds a predetermined threshold; and

the sending verification method information to the second mobile device comprises the following:

sending the verification method information to the second mobile device if the account credit information corresponding to the second mobile device exceeds the predetermined threshold.

4. The method according to any one of claims 1 or 2, wherein after sending enabling information of the second mobile device to the second mobile device, the method further comprises the following:

generating token information corresponding to the first mobile device identifier information; and

sending the token information to the second mobile device.

5. The method according to claim 4, wherein the payment information sent by the second mobile device further comprises the token information and a device certificate of the first mobile device, and before obtaining account information corresponding to the first mobile device

identifier information, the method further comprises the following:

separately verifying whether the token information and the device certificate of the first mobile device are correct; and

obtaining account information corresponding to the first mobile device identifier information comprises the following:

obtaining the account information corresponding to the first mobile device identifier information if both the token information and the device certificate of the first mobile device are correct.

6. The method according to claim 5, wherein after separately verifying whether the token information and the device certificate of the first mobile device are correct, the method further comprises the following:

sending identity authentication failure prompt information of the first mobile device to the second mobile device if it is verified that either the token information or the device certificate of the first mobile device is incorrect.

7. The method according to any one of claims 1 to 6, wherein the token is stored for a set time interval after being generated and is automatically deleted after the set time interval.

8. The method according to any one of claims 1 to 7, wherein the certificate of the first mobile device is stored in security zones of the first mobile device and the second mobile device; and/or wherein the certificate of the first mobile device is sent to a third-party server for identity authentication.

9. The method according to any one of claims 1 to 8, wherein the account information is obtained based on historical payment information of the first mobile device.

10. A device for mobile payment, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 9.