

CLAIMS

What is claimed is:

1. A payment service implementation method, applied to a terminal that performs a payment service, wherein the method comprises:

- 5 generating a random number;
- encrypting original payment account information of the terminal by using the random number as a key of a second encryption algorithm, to obtain second payment account information;
- performing first combination processing on the random number and the second
- 10 payment account information to obtain transformed payment account information;
- encrypting the transformed payment account information according to a public key and a first encryption algorithm obtained in advance, to obtain first payment account information;
- obtaining anonymous payment account information according to the first payment
- 15 account information; and
- performing a payment operation by using the anonymous payment account information.

2. The method according to claim 1, wherein

- the generating a random number comprises: generating, according to a key length
- 20 of a second encryption algorithm, the random number whose length is equal to the key length.

3. The method according to claim 1, wherein

- the obtaining anonymous payment account information according to the first payment account information comprises:
- 25 directly determining the first payment account information as the anonymous payment account information.

4. The method according to any one of claims 1 to 3, wherein the terminal that performs a payment service is a terminal that provides payment account information; and

- 30 the performing a payment operation by using the anonymous payment account information comprises:
- providing the anonymous payment account information to another terminal.

5. The method according to any one of claims 1 to 3, wherein the terminal that performs a payment service is a terminal that provides a payment bill to a server; and the performing a payment operation by using the anonymous payment account information comprises:

5 generating an anonymous payment bill by using the anonymous payment account information; and

 sending the anonymous payment bill to the server.

6. A payment service implementation method, applied to a server and comprising: receiving an anonymous payment bill;

10 obtaining anonymous payment account information from the anonymous payment bill;

 performing decryption processing by using a predetermined private key, a first decryption algorithm, and the anonymous payment account information, to obtain transformed payment account information, wherein the private key corresponds to a public key obtained by a terminal that performs a payment service;

15 obtaining a random number;

 performing inverse transform processing on the transformed payment account information by using the random number to obtain original payment account information; and

20 performing bill deduction processing according to the original payment account information.

7. The method according to claim 6, wherein the transformed payment account information does not carry the random number;

 the obtaining a random number comprises: performing second de-combination processing on the anonymous payment account information, and extracting the random number from payment account information obtained after the second de-combination processing; and

 the performing decryption processing by using a predetermined private key, a first decryption algorithm, and the anonymous payment account information comprises:

30 extracting first payment account information from the payment account information obtained after the second de-combination processing; and

 decrypting the first payment account information by using the private key and the first decryption algorithm.

8. The method according to claim 6, wherein the transformed payment account

information carries the random number;

the performing decryption processing by using a predetermined private key, a first decryption algorithm, and the anonymous payment account information comprises: decrypting the anonymous payment account information by using the private key and
5 the first decryption algorithm; and

the obtaining a random number comprises: performing first de-combination processing on the decrypted payment account information, and extracting the random number from payment account information obtained after the first de-combination processing.

10 9. A payment service implementation apparatus, disposed in a terminal that performs a payment service, wherein the apparatus comprises:

a random number generation unit, configured to generate a random number;

a transform processing unit, configured to encrypt original payment account
15 information of the terminal by using the random number, as a key of a second encryption algorithm, to obtain second payment account information, and perform first combination processing on the random number and the second payment account information to obtain transformed payment account information;

an encryption processing unit, configured to encrypt the transformed payment
20 account information according to a public key and a first encryption algorithm obtained in advance, to obtain first payment account information;

an anonymous account determining unit, configured to obtain anonymous payment account information according to the first payment account information; and

a payment processing unit, configured to perform a payment operation by using
25 the anonymous payment account information.

10. The apparatus according to claim 9, wherein

the random number generation unit is configured to generate, according to a key length of a second encryption algorithm, the random number whose length is equal to the key length.

30 11. The apparatus according to claim 9, wherein

the anonymous account determining unit is configured to:

directly determine the first payment account information as the anonymous payment account information.

12. The apparatus according to any one of claims 9 to 11, wherein the terminal that

performs a payment service is a terminal that provides payment account information;
and

the payment processing unit is configured to:

provide the anonymous payment account information to another terminal.

5 13. The apparatus according to any one of claims 9 to 11, wherein the terminal that
performs a payment service is a terminal that provides a payment bill to a server; and
the payment processing unit is configured to:

generate an anonymous payment bill by using the anonymous payment account
information; and

10 send the anonymous payment bill to the server.

14. A server, comprising:

a receiving unit, configured to receive an anonymous payment bill;

an account obtaining unit, configured to obtain anonymous payment account
information from the anonymous payment bill;

15 a decryption processing unit, configured to perform decryption processing by
using a preset private key, a first decryption algorithm, and the anonymous payment
account information, to obtain transformed payment account information, wherein the
private key corresponds to a public key obtained by a terminal that performs a payment
service;

20 a random number acquisition unit, configured to obtain a random number;

an inverse transform processing unit, configured to perform inverse transform
processing on the transformed payment account information by using the random
number to obtain original payment account information; and

25 a deduction processing unit, configured to perform bill deduction processing
according to the original payment account information.

15. The server according to claim 14, wherein the transformed payment account
information does not carry the random number;

30 the random number obtaining unit is configured to: perform second de-
combination processing on the anonymous payment account information, and extract
the random number from payment account information obtained after the second de-
combination processing; and

the decryption processing unit is configured to:

extract first payment account information from the payment account information
obtained after the second de-combination processing; and

decrypt the first payment account information by using the private key and the first decryption algorithm.

16. The server according to claim 14, wherein the transformed payment account information carries the random number;

5 the decryption processing unit is configured to decrypt the anonymous payment account information by using the private key and the first decryption algorithm; and

 the random number obtaining unit is configured to: perform first de-combination processing on the decrypted payment account information, and extract the random number from payment account information obtained after the first de-combination processing.

10

17. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 8.