

WHAT IS CLAIMED IS:

1. A method of applying for a payment token, applicable to a second application module at a terminal device, comprising:

5 displaying bound payment accounts upon receiving an invocation instruction from a first application module, for a user to select one from the bound payment accounts, wherein the invocation instruction carries merchant information of the first application module; and

10 sending to a server an authorization request for token binding, for the first application module to apply to the server for a payment token based on an authorization code for token binding returned by the server, wherein the authorization request for token binding carries the merchant information of the first application module and the payment account selected by the user, and the server generates the payment token if validation of a payment token request passes, and sends the payment token to the first application
15 module.

2. The method according to claim 1, wherein the authorization request for token binding further carries transaction control parameters.

3. The method according to claim 2, wherein the transaction control parameters comprise at least one selected from a validity period of the payment token, a transaction
20 volume limit per day of the payment token and the maximum number of transactions per day of the payment token.

4. The method according to claim 2, further comprising providing a setting interface for the user to set the transaction control parameters.

5. The method according to claim 1, further comprising receiving the authorization code
25 for token binding from the server and forwarding the received authorization code for token binding to the first application module.

6. The method according to claim 5, wherein information for confirmation prompt on the payment account and/or on the user's identification is further sent to the first application module while forwarding the received authorization code for token binding to
30 the first application module.

7. A method of applying for a payment token, applicable to a first application module at

a terminal device, comprising:

invoking a second application module, and transmitting merchant information of the first application module to the second application module, for the second application module to send to a server an authorization request for token binding, wherein the authorization request for token binding carries the merchant information of the first application module and a payment account selected by a user from the second application module, the first application module is a software for invoking the second application module, and the payment accounts selectable by the user are bound beforehand by the user to the second application module;

receiving an authorization code for token binding generated by the server in response to the authorization request for token binding;

sending to the server a payment token request carrying the authorization code for token binding; and

receiving a payment token from the server.

8. The method according to claim 7, wherein the authorization code for token binding is forwarded by the second application module from the server to the first application module;

information for confirmation prompt on the payment account and/or on the user's identification is further received from the second application module while receiving the authorization code for token binding from the second application module; and

the method further comprises: displaying the information for confirmation prompt on the payment account and/or on the user's identification to prompt the user to confirm whether the information for confirmation prompt is correct; and

sending the payment token request to the server if the user confirms that the information for confirmation prompt is correct.

9. The method according to claim 7, further comprising selecting the second application module, which comprises:

sending a query request to the server to query application modules supported by the server; and

displaying a list of the queried application modules for the user to select an

application module therefrom as the second application module.

10. The method according to claim 7, wherein an encrypted authentication code and the merchant information of the first application module are further sent to the server if the second application module is invoked, wherein the encrypted authentication code is a ciphertext of the merchant information of the first application module as acquired by the first application module upon registering with the server.

11. The method according to claim 7, further comprising:

receiving from the server first encrypted data, a second secret key and clock information, wherein the first encrypted data is a ciphertext acquired by encrypting the authorization code for token binding with the first secret key;

synchronizing a local clock according to the received clock information, and acquiring second encrypted data by encrypting the merchant information with the second secret key and the synchronized clock; and

further sending the second encrypted data and the first encrypted data to the server if the second application module is invoked.

12. A method of applying for a payment token, applicable to a server, comprising:

receiving from a second application module an authorization request for token binding, wherein the authorization request for token binding carries merchant information of a first application module, and a payment account selected by a user from bound payment accounts of the second application module;

generating an authorization code for token binding if validation of the authorization request for token binding passes, and sending the authorization code for token binding to the first application module;

receiving from the first application module a payment token request carrying the authorization code for token binding; and

generating a payment token if validation of the payment token request passes, and sending the payment token to the first application module.

13. The method according to claim 12, wherein the authorization request for token binding further carries merchant information of the first application module; and

validation of the authorization request for token binding passes if the merchant

information carried by the authorization request for token binding is information of a merchant registered with the server.

14. The method according to claim 12, further comprising:

providing a registration service to the first application module;

5 encrypting the merchant information of the first application module to acquire an encrypted authentication code;

sending the encrypted authentication code to the first application module;

receiving from the first application module the encrypted authentication code and the merchant information; and

10 decrypting the encrypted authentication code, comparing a resulting plaintext to the received merchant information, and determining that validation of the authorization request for token binding passes if the plaintext and the merchant information are consistent.

15 15. The method according to claim 12, wherein the payment token request further carries the merchant information of the first application module, and validation of the payment token request comprises at least one selected from following three validation methods:

determining that the validation passes if the authorization code for token binding exists;

20 determining that the validation passes if the merchant information is consistent with that carried by the authorization request for token binding; and

determining that the validation passes if the authorization code for token binding is within a validity period.

25 16. The method according to claim 12, wherein first encrypted data, a second secret key and clock information are further sent to the first application module while generating the authorization code for token binding, wherein the first encrypted data is a ciphertext acquired by encrypting the authorization code for token binding with a first secret key; and

the method further comprises:

receiving from the first application module second encrypted data and the first encrypted data; and

acquiring a third encrypted data by encrypting the merchant information of the first application module with the second secret key and the clock information, determining whether the third encrypted data is consistent with the second encrypted data received from the first application module, determining whether a result acquired by decrypting the received first encrypted data with the first secret key is consistent with the authorization code for token binding, and if both determination results are consistent, determining that validation of the payment token request passes.

17. The method according to claim 12, wherein sending the authorization code for token binding to the first application module comprises sending the authorization code for token binding to the first application module by forwarding via the second application module.

18. A method of applying for a payment token, comprising:

at a terminal device, invoking, by a first application module, a second application module, and transmitting merchant information of the first application module to the second application module;

at the terminal device, displaying, by the second application module, bound payment accounts in the second application module upon receiving an invocation instruction from the first application module, for a user to select one from the bound payment accounts, and sending an authorization request for token binding to a server, wherein the authorization request for token binding carries the merchant information of the first application module and the payment account selected by the user;

generating, by the server, an authorization code for token binding if validation of the authorization request for token binding passes, and sending the authorization code for token binding to the first application module;

at the terminal device, sending, by the first application module, a payment token request to the server, wherein the payment token request carries the authorization code for token binding; and

generating, by the server, a payment token if validation of the payment token request passes, and sending the payment token to the first application module.

19. A terminal device, comprising a first memory and a first processor, the first memory having a first instruction and/or a second instruction stored therein, wherein the first instruction, when executed by the first processor, causes the method of applying for a payment token according to any one of claims 7-11 to be performed, and the second
5 instruction, when executed by the first processor, causes the method of applying for a payment token according to any one of claims 1-6 to be performed.

20. A server, comprising a second memory and a second processor, the second memory having a payment token managing program stored therein, wherein the payment token managing program, when executed by the second processor, causes the
10 method of applying for a payment token according to any one of claims 12-17 to be performed.

21. A system for applying for a payment token, comprising the terminal device according to claim 19 and the server according to claim 20.