

What is claimed is:

1. A card management method, applicable to a user terminal, the user terminal including a security element which stores first-type universal personalization data which is a first part of personalization data for transaction verification of a first type of cards and second-type universal personalization data which is a first part of personalization data for transaction verification of a second type of cards, different cards of the first type share the same first-type universal personalization data and different cards of the second type share the same second-type universal personalization data, the method comprising:

sending, to a server, a card binding message including card authentication information of a card to be bound in an application of the user terminal such that the server determines a card type of the card and allocates dedicated card information for the card in a case of successful verification of the card, wherein the dedicated card information comprises a card transaction identifier and dedicated personalization data for the card, the card transaction identifier being a token for the card and the dedicated personalization data for the card being a second part of personalization data for transaction verification of the card;

receiving the card type of the card and the dedicated card information for the card sent by the server, without need to download corresponding universal personalization data for the card from the server; and

loading the dedicated card information for the card onto the security element to bind the card in the application, wherein the dedicated card information for the card together with one of the first-type universal personalization data and the second-type universal personalization data that are stored in the security element and matches the card type are useable to perform transaction verification of the card.

2. The method according to claim 1, wherein in a case that the card to be bound comprises a first card and a second card with a same card type, the dedicated card information for the first card together with one of the first-type universal personalization data and the second-type universal personalization data that are stored in the security element and matches the card type are useable to perform transaction verification of the first card, and the dedicated card information for the second card together with one of the first-type universal personalization data and the second-type universal personalization data that are stored in the security element and matches the card type are useable to perform transaction verification of the second card.

3. The method according to claim 1, further comprising setting a life state of the card to a valid state through the security element, and generating or updating a first mapping relationship, wherein the first mapping relationship comprises a mapping relationship among the dedicated card information for the card, the card type of the card, and the life state of the card.

4. The method according to claim 3, further comprising synchronizing the set life state of the card and the first mapping relationship to the server.

5. The method according to claim 1, wherein the card binding message comprises a first card binding message, a second card binding message and a binding verification message, and the card authentication information comprises a card identifier of the card, card type verification information corresponding to the card type of the card and an input verification code; and

wherein the sending of the card binding message to the server comprises:

sending the first card binding message to the server, the first card binding message comprising the card identifier of the card;

sending the second card binding message to the server upon reception of a first response message sent by the server, the first response message comprising the card type of the card, and the second card binding message comprising the card type verification information corresponding to the card type of the card; and

sending the binding verification message to the server upon reception of a second response message sent by the server, the second response message comprising a dynamic verification code, and the binding verification message comprising the input verification code.

6. The method according to claim 1, wherein in a case that the user terminal performs card binding for the first time, the method further comprises:

receiving a universal program data package sent by the server; and

loading the universal program data package onto the security element.

7. The method according to claim 3, further comprising:

receiving a default card selection input which indicates a selected default card from multiple cards which have been bound;

controlling the security element to update a life state of an original default card to a valid state, wherein the life state of the original default card before being updated is a default use state;

controlling the security element to update a life state of the selected default card to the default use state; and

synchronizing the updated life state of the selected default card and the updated life state of the original default card to the server.

8. The method according to claim 3, further comprising:

sending a card deleting request message to the server such that the server feeds back a card transaction identifier of a card to be deleted among multiple cards which have been bound, the card deleting request message indicating the card to be deleted;

receiving the card transaction identifier of the card to be deleted fed back by the server;

controlling the security element to update a life state of the card to be deleted to an invalid state; and

synchronizing the updated life state of the card to be deleted to the server.

9. The method according to claim 8, wherein after the receiving of the card transaction identifier of the card to be deleted fed back by the server, the method further comprises:

deleting a second mapping relationship through the security element, the second mapping relationship comprising a mapping relationship among dedicated card information for the card to be deleted, a card type of the card to be deleted, and the life state of the card to be deleted.

10. A card management method, applicable to a server, the server storing first-type universal personalization data which is a first part of personalization data for transaction verification of a first type of cards and second-type universal personalization data which is a first part of personalization data for transaction verification of a second type of cards, different cards of the first type share the same first-type universal personalization data and different cards of the second type share the same second-type universal personalization data, the method comprising:

determining a card type of a card to be bound in an application of a user terminal and verifying the card in response to a received card binding message sent by the user terminal, and allocating dedicated card information to the card in a case of successful verification of the card, wherein the card binding message comprises card authentication information of the card, the dedicated card information comprises a card transaction identifier and dedicated personalization data for the card, the card transaction identifier being a token for the card and the dedicated personalization data for the card being a second part of personalization data for transaction verification of the card, the dedicated card information for the card together with one of the first-type universal personalization data and the second-type universal personalization data that matches the card type are useable to perform transaction verification of the card; and

sending a card binding response message to the user terminal, the card binding response message comprising the card type of the card and the dedicated card information for the card.

11. The method according to claim 10, wherein in a case that the card to be bound comprises a first card and a second card with a same card type, the dedicated card information for the first card together with one of the first-type universal personalization data and the second-type universal personalization data that matches the card type are useable to perform transaction verification of the first card, and the dedicated card information for the second card together with one of the first-type universal personalization data and the second-type universal personalization data that are stored in the security element and matches the card type are useable to perform transaction verification of the second card.

12. The method according to claim 10, further comprising keep synchronization with the user terminal in a life state of the card and a first mapping relationship, the first mapping relationship comprising a mapping relationship among the dedicated card information for the card, the card type of the card and the life state of the card.

13. The method according to claim 10, wherein the card binding response message comprises a first response message, a second response message and a third response message, and the card authentication information comprises a card identifier of the card, card type verification information corresponding to the card type of the card and an input verification code;

wherein the sending of the card binding response message to the server comprises:

sending the first response message to the user terminal upon determining the card type of the card in response to a first card binding message sent by the user terminal, the first response message comprising the card type of the card, and the first card binding message comprising the card identifier of the card;

sending the second response message to the user terminal in a case of successful verification of the card type of the card in response to a second card binding message sent by the user terminal, the second card binding message comprising the card type verification information that matches the card type of the card, and the second response message comprising a dynamic verification code; and

sending the third response message to the user terminal in a case of successful verification of a verification code of the card in response to a binding verification message sent by the user terminal, the binding verification message comprising the input verification code, and the third response message comprising the dedicated card information for the card.

14. The method according to claim 13, wherein the card binding message comprises the first card binding message, the second card binding message and the binding verification message;

wherein the determining of the card type of the card, verifying of the card in response to the card binding message sent by the user terminal and allocating of the dedicated card information for the card in a case of successful verification of the card comprises:

determining the card type of the card according to the card identifier of the card in the first card binding message;

performing card type verification on the card using the card type verification information of the card in the second card binding message; and

allocating the dedicated card information for the card in a case that the input verification code in the binding verification message is consistent with the dynamic verification code.

15. The method according to claim 10, wherein in a case that the user terminal performs card binding for the first time, the method further comprises sending a universal program data package to the user terminal.

16. The method according to claim 10, further comprising keep in synchronization with the user terminal in an updated life state of a default card and an updated life state of an original default card, wherein a life state of the original default card before being updated is a default use state.

17. The method according to claim 10, further comprising feeding back a card transaction identifier of a card to be deleted among multiple cards that have been bounded in the application of the user terminal in response to a card deleting request message sent by the user terminal, the card deleting request message indicating the card to be deleted; and

keeping in synchronization with the user terminal in an updated life state of the card to be deleted.

18. The method according to claim 17, further comprising deleting a second mapping relationship, wherein the second mapping relationship comprises a mapping relationship among dedicated card information for the card to be deleted, a card type of the card to be deleted, and the life state of the card to be deleted.

19. A user terminal, comprising a security element which stores first-type universal personalization data which is a first part of personalization data for transaction verification of a card of a first type and second-type universal personalization data which is a first part of personalization data for transaction verification of a card of a second type, different cards of the first type share the same first-type universal personalization data and different cards of the second type share the same second-type universal personalization data;

wherein the user terminal comprises:

a sending module configured to send, to a server, a card binding message including card authentication information of a card to be bound in an application of the user terminal such that the server determines a card type of the card, and in a case of successful verification of the card, allocates dedicated card information for the card in a case of successful verification of the card, wherein the dedicated card information comprises a card transaction identifier and dedicated personalization data for the card, the card transaction identifier being a token for the card and the dedicated personalization data for the card being a second part of personalization data for transaction verification of the card;

a receiving module configured to receive the card type of the card and the dedicated card information for the card sent by the server, without need to download corresponding universal personalization data for the card from the server; and

a processing module configured to load the dedicated card information for the card onto the security element to bind the card in the application, wherein the dedicated card information for the card together with one of the first-type universal personalization data and second-type universal personalization data that are stored in the security element and matches the card type are useable to perform transaction verification of the card to be bound.

20. A server storing first-type universal personalization data which is a first part of personalization data for transaction verification of a card of a first type and second-type universal personalization data which is a first part of personalization data for transaction verification of a card of a second type, different cards of the first type share the same first-type universal personalization data and different cards of the second type share the same second-type universal personalization data;

wherein the server comprises:

a receiving module configured to receive a card binding message sent by a user terminal, wherein the card binding message comprises card authentication information of a card to be bound in an application of a user terminal;

a processing module configured to determine a card type of the card and verify the card in response to the card binding message, and allocate dedicated card information to the card in a case of successful verification of the card, wherein the dedicated card information comprises a card transaction identifier and dedicated personalization data for the card, the card transaction identifier being a token for the card and the dedicated personalization data for the card being a second part of personalization data for transaction verification of the card, the dedicated card information for the card together with one of the first-type universal personalization data and the second-type universal personalization data that matches the card type are useable to perform transaction verification of the card; and

a sending module configured to send a card binding response message to the user terminal, wherein the card binding response message comprises the card type of the card and the dedicated card information for the card.

21. A user terminal, comprising a processor and a memory storing computer program instructions, wherein the processor executes the computer program instructions to implement the card management method according to any one of claims 1 to 9.

22. A server, comprising a processor and a memory storing computer program instructions, wherein the processor executes the computer program instructions to implement the card management method according to any one of claims 10 to 18.

23. A card management system, comprising the user terminal according to claim 19 and the server according to claim 20.

24. A computer storage medium, storing computer program instructions, wherein the computer program instructions are executed by a processor to perform the card management method according to any one of claims 1 to 18.