

DATA INTERACTION METHOD AND SYSTEM

FIELD

The present disclosure relates to electronic information security technology field,
5 and more particularly to a data interaction method and a data interaction system.

BACKGROUND

During transaction process in the related art, such as withdrawal or purchasing by
cards, users usually need to carry bank cards got from banks with them, which may
10 have a certain security risk. Once the bank card is lost, it is easy to result in loss to the
user's assets. In addition, due to the various types of bank cards, a user may
simultaneously have multiple bank cards from different banks. It is not convenient if all
the plurality of bank cards from different banks are carried with the user. If for
convenience, only some of the plurality of bank cards from different banks are carried
15 with the user, there may be inter-bank transactions when using these bank cards for
withdrawal or purchasing by cards, which may result in unnecessary costs incurred in
the transaction.

Therefore, there is an urgent need to provide a transaction solution that is
convenient for the user's carrying and has high security.

20

SUMMARY

The present disclosure seeks to solve the above problems.

An objective of the present disclosure is to provide a data interaction method.

In order to achieve the above objective, technical solutions of the present
25 disclosure are specifically realized as follows.

According to an aspect of the present disclosure, a data interaction method is
provided. The method includes: obtaining a real card information list of smart cover end
by a smart cover, wherein the real card information list of smart cover end is a real card
information list of real card manager end obtained by the smart cover from a real card
30 manager, and the real card information list of real card manager end includes real card

information of real cards connected to the real card manager; prompting the real card information list of smart cover end by the smart cover; receiving a real card selecting instruction by the smart cover, determining a selected real card by the card sheath, and receiving first data sent from a transaction terminal by a simulation card, and sending
5 the first data to the smart cover by the simulation card; prompting the first data by the smart cover, receiving a confirming instruction for confirming that the first data is correct by the smart cover, and sending the first data to the real card manager by the smart cover; and receiving the first data sent from the smart cover by the real card manager, and sending the first data to the selected real card by the real card manager.

10 In addition, the data interaction method further includes: establishing a secure connection between the smart cover and the simulation card, and obtaining a first secure transmission key of smart cover end and a secure transmission key of simulation card end for secure data transmission between the smart cover and the simulation card.

In addition, the data interaction method further includes: establishing a secure
15 connection between the smart cover and the real card manager, and obtaining a second secure transmission key of smart cover end and a secure transmission key of real card manager end for secure data transmission between the smart cover and the real card manager.

In addition, before establishing a secure connection between the smart cover and
20 the simulation card, the data interaction method further includes: performing a binding operation between the smart cover and the simulation card.

In addition, before establishing a secure connection between the smart cover and the simulation card, the data interaction method further includes: performing a binding operation between the smart cover and the real card manager.

25 In addition, before establishing a secure connection between the smart cover and the real card manager, the data interaction method further includes: sending a login request to the real card manager by the smart cover; and after establishing a secure connection between the smart cover and the real card manager, further includes: performing a first processing on a received login password by the smart cover using the
30 second secure transmission key of smart cover end to obtain a first processed password,

and sending the first processed login password to the real card manager by the smart cover; receiving data sent from the smart cover by the real card manager, performing a second processing on received data by the real card manager using the secure transmission key of real card manager end to obtain second processed data, and
5 verifying a correctness of the second processed data by the real card manager; after the real card manager verifies that the second processed data passes verification, making the smart cover login to the real card manager.

In addition, wherein performing a second processing on received data by the real card manager using the secure transmission key of real card manager end to obtain
10 second processed data and verifying a correctness of the second processed data by the real card manager includes: performing the second processing on the received data by the real card manager using the secure transmission key of real card manager end to obtain a password to be verified; determining, by the real card manger, whether the password to be verified is an alarm password; if the password to be verified is an alarm
15 password, performing an alarm operation by the real card manager after verified the password to be verified successful; if the password to be verified is a login password rather than an alarm password, determining that the password to be verified passes the verification by the real card manager.

In addition, the data interaction method further includes: detecting, by the real card
20 manager, the real cards connected to the real card manager; after the real card manager detects the real cards connected to the real card manager, obtaining real card information of the real cards by the real card manager, wherein the real card information includes at least a card number; after the real card manager obtains the real card information of the real cards, generating the real card information list of real card
25 manager end by the real card manager.

In addition, the data interaction method further includes: generating an identification list of real card manager end by the real card manager, wherein identifications in the identification list of real card manager end have a one-to-one correspondence with the real card information in the real card information list of real
30 card manager end.

In addition, receiving a real card selecting instruction by the smart cover and determining a selected real card by the smart cover includes: receiving the real card selecting instruction by the smart cover, and obtaining a selected identification by the smart cover, in which the selected identification is configured to indicate the selected
5 real card; sending the selected identification to the real card manager by the smart cover; determining the selected real card corresponding to the selected identification by the real card manager from the real cards connected to the real card manager according to the selected identification.

10 In addition, the real card manager sets ON and/or OFF for read and write access to the real card information of the real cards connected to the real card manager according to security levels of the real cards.

In addition, the smart cover is a mobile device.

In addition, the smart cover is a combination of a mobile device and an electronic
15 signature token, or the smart cover is an electronic signature token.

Another objective of the present disclosure is to provide a data interaction system.

In order to achieve the above objective, technical solutions of the present disclosure are specifically realized as follows.

According to another aspect of the present disclosure, a data interaction system is
20 provided. The system includes a simulation card, a smart cover and a real card manager. The smart cover is configured to obtain a real card information list of smart cover end, to prompt the real card information list of smart cover end, to receive a real card selecting instruction, and to determine a selected real card, in which the real card information list of smart cover end is a real card information list of real card manager
25 end obtained by the smart cover from the real card manager, and the real card information list of real card manager end includes real card information of real cards connected to the real card manager. The simulation card is configured to receive first data sent by a transaction terminal, and to send the first data to the smart cover. The smart cover is further configured to prompt the first data, to receive a confirming
30 instruction for confirming that the first data is correct, and to send the first data to the

real card manager. The real card manager is configured to receive the first data sent by the smart cover, and to send the first data to the selected real card.

It can be seen from the above technical solutions of the present disclosure that, with the data interaction method and the data interaction system, data interaction among the simulation card, the smart cover and the real card manager can be realized, thus
5 providing a new transaction solution that is not only convenient for the user's carrying but also has high security.

BRIEF DESCRIPTION OF THE DRAWINGS

10 In order to make technique solutions according to embodiments of the present disclosure more apparent, drawings needed to be used in descriptions of the embodiments will be illustrated in the following. Obviously, the drawings to be illustrated in the following only represent some embodiments of the present disclosure, and other drawings can be obtained according these drawings by skilled in the art
15 without making creative labors.

Fig. 1 is a flow chart of a data interaction method according to an embodiment of the present disclosure;

Fig. 2 shows a block diagram of a data interaction system according to an embodiment of the present disclosure;

20 Fig. 3 is a flow chart of a first data updating method according to an embodiment of the present disclosure;

Fig. 4 is a flow chart of a second data updating method according to an embodiment of the present disclosure;

25 Fig. 5 is a flow chart of a third data updating method according to an embodiment of the present disclosure;

Fig. 6 is a flow chart of a fourth data updating method according to an embodiment of the present disclosure;

30 Fig. 7 is a flow chart of a first manner for establishing a secure connection between a smart cover and a simulation card according to an embodiment of the present disclosure;

Fig. 8 is a flow chart of a second manner for establishing a secure connection between a smart cover and a simulation card according to an embodiment of the present disclosure;

Fig. 9 is a flow chart of a first manner for establishing a secure connection between a smart cover and a real card manager according to an embodiment of the present disclosure;

Fig. 10 is a flow chart of a second manner for establishing a secure connection between a smart cover and a real card manager according to an embodiment of the present disclosure;

Fig. 11 is a flow chart of performing a binding operation between a smart cover and a simulation card according to an embodiment of the present disclosure;

Fig. 12 is a flow chart of performing a binding operation between a smart cover and a real card manager according to an embodiment of the present disclosure;

Fig. 13 is a flow chart of updating an application of a smart cover according to an embodiment of the present disclosure;

Fig. 14 is a flow chart of updating an application of a simulation card according to an embodiment of the present disclosure;

Fig. 15 is a flow chart of updating an application of a real card manager according to an embodiment of the present disclosure.

DETAILED DESCRIPTION

Technical solutions of embodiments of the present disclosure will be described clearly and completely with reference to the drawings, and obviously, only part of embodiments are described herein. All other embodiments may be obtained by those skilled in the art based on the embodiments described, without any creative effort, and belong to the protection scope of the present disclosure.

In the description of the present disclosure, it should be understood that terms such as “central,” “longitudinal,” “lateral,” “upper,” “lower,” “front,” “rear,” “left,” “right,” “vertical,” “horizontal,” “top,” “bottom,” “inner,” and “outer,” should be construed to refer to the orientation as then described or as shown in the drawings under discussion.

These relative terms are for convenience of description and do not require that the present disclosure be constructed or operated in a particular orientation. In addition, terms such as “first” and “second” are used herein for purposes of description and are not intended to indicate or imply relative importance or significance.

5 In the description of the present disclosure, it should be noted that, unless specified or limited otherwise, the terms “mounted,” “connected,” and “coupled” and the like are used broadly, and may be, for example, fixed connections, detachable connections, or integral connections; may also be mechanical or electrical connections; may also be direct connections or indirect connections via intervening structures; may also be inner
10 communications of two elements, which can be understood by those skilled in the art according to specific situations.

Embodiments of the present disclosure will be further described in detail with reference to the drawings.

 The present disclosure provides a data interaction architecture, so as to provide a
15 transaction solution that is not only convenient for users’ carrying, but also has high security. The data interaction architecture includes a simulation card, a smart cover, and a real card manager.

 There may be one or more simulation cards. The simulation card may be a card that is individually manufactured or a real card having a reserved simulation card
20 function. The simulation card has the same size as an existing bank card, and replaces real cards to complete transaction in the present data interaction architecture. The simulation card has a contact interface and/or a contactless interface, so as to complete transaction in cooperation with an existing transaction terminal (such as an ATM (Automatic Teller Machine), a POS, and a recharge machine for bus cards). The
25 simulation card may also have a wireless interface, and the simulation card can perform data interaction with the smart cover via this wireless interface. The contact interface may include contacts, and the contactless interface may be an NFC (Near Field Communication) interface, and the wireless interface may be a Bluetooth interface, an infrared interface, a 2.4GHz interface, a WIFI interface or a RFID (Radio Frequency
30 Identification Devices) interface.

There may be one or more smart covers. Each smart cover may manage one or more simulation cards. Each simulation card belongs to and is managed by only one smart cover. The smart cover may be an individually manufactured device having a shape of a card holder, or a mobile device with a function of the smart cover in the present data interaction architecture, including a smart phone, a tablet computer (such as a PAD), a PDA (such as a palmtop, a learning machine), a laptop, an electronic book reading device, a wearable device (such as a smart watch, smart glasses) and the like. The smart cover may include a contact interface and/or a contactless interface, so as to perform data interaction in cooperation with the contact interface and/or the contactless interface of the simulation card. The smart cover may also include a wireless interface, so as to perform data interaction with corresponding interface of the simulation card via this wireless interface. The contact interface may include contacts, and the contactless interface may be an NFC interface, and the wireless interface may be a Bluetooth interface, an infrared interface, a 2.4GHz interface, a WIFI interface or a RFID interface. The smart cover may also include a network interface, so as to perform data interaction with corresponding network interface of the real card manager via this network interface. The network interface may be a WIFI interface, a mobile internet interface (such as 3G network and 4G network). In addition, the smart cover may also be a combination of the mobile device and an electronic signature token, in which the network interface of the smart cover is realized by the network interface of the mobile device, and other interfaces (such as the wireless interface, the contact interface and/or the contactless interface) may be located in the electronic signature token, or the other interfaces may also be located in the mobile device, or some of the other interfaces may be located in the electronic signature token and some of the other interfaces may be located in the mobile device. All the processing operations performed by the smart cover are performed on the electronic signature token. The smart cover may also be the electronic signature token only. The electronic signature token may be a key device, such as a U type shield of Industrial and Commercial Bank of China and a USB-key of Agricultural Bank of China.

The real card manager can manage multiple smart covers. The real card manager

includes multiple contact interfaces (such as card slots) and/or contactless interfaces (such as NFC interfaces), so as to facilitate that the real card manager can be connected to different types of real cards in different ways. The real card manager is connected to at least one real card, and stores a real card information list of real card manager end.

5 The real card information list of real card manager end includes real card information of real cards that are connected to the real card manager. The real card information may include information such as card numbers and card authentication information and so on. The card authentication information is card information used to authenticate whether a real card is issued by a regular channel (such as banks and bus companies). The real
10 card may be a function card (such as a bus card, a dining card, a shopping card, a membership card, a scorecard, etc.) or a bank card issued by a bank. Alternatively, the real card manager may be set to store real card information of all or part of the real cards that are connected to the real card manager, so that a user can make different settings according to security requirements of the real cards. For example, it can be set
15 in the real card manager that obtaining real card information of some real cards is not allowed, thus ensuring security of these real cards. The real card manager may also include a network interface, so as to perform data interaction with corresponding network interface of the smart cover via this network interface. The network interface may be a WIFI interface, a mobile internet interface (such as 3G network and 4G
20 network), or the like.

In the present data interaction architecture, both the simulation card and the real cards are smart chip cards.

Terms in the present disclosure are explained as follows.

A first processing includes an encryption processing, and a second processing
25 includes a decryption processing. Specifically, encryption alone ensures security of data transmission. When security level of data to be transmitted is required high, this way can be used to process the data to be transmitted.

Or, the first processing includes a verification calculating processing, and the second processing includes a verification validation calculating processing. Specifically,
30 verification alone ensures integrity of data transmission, preventing tampering. When

integrity level of the data to be transmitted is required high, this way can be used to process the data to be transmitted.

Or, the first processing includes an encryption and verification calculating processing, and the second processing includes a decryption and verification validation calculating processing. Specifically, security and integrity of data transmission are ensured by using a combination of the encryption and the verification. When security level of the data to be transmitted is required the highest, this way can be used to process the data to be transmitted.

Based on the above data interaction architecture, with the data interaction method according to the present disclosure, data interaction among the simulation card, the smart cover and the real card manager can be realized, thus providing a new transaction solution that is not only convenient for the user's carrying but also has high security.

Fig. 1 is a flow chart of a data interaction method according to an embodiment of the present disclosure. Referring to Fig. 1, the data interaction method according to the present disclosure includes following operations.

The smart cover obtains a real card information list of smart cover end. The real card information list of smart cover end is a real card information list of real card manager end that the smart cover obtains from the real card manager. The real card information list of real card manager end includes real card information of real cards that are connected to the real card manager.

The smart cover prompts the real card information list of smart cover end.

The smart cover receives a real card selecting instruction, and determines a selected real card. The simulation card receives first data sent by a transaction terminal, and sends the first data to the smart cover.

The smart cover prompts the first data, and receives a confirming instruction for confirming that the first data is correct, and sends the first data to the real card manager.

The real card manager receives the first data sent by the smart cover, and sends the first data to the selected real card.

Fig. 2 shows a block diagram of a data interaction system according to an embodiment of the present disclosure. Referring to Fig. 2, the data interaction system

according to the present disclosure includes a simulation card, a smart cover, and a real card manager.

5 The smart cover is configured to obtain a real card information list of smart cover end, to prompt the real card information list of smart cover end, to receive a real card selecting instruction, and to determine a selected real card. The real card information list of smart cover end is a real card information list of real card manager end that the smart cover obtains from the real card manager, and the real card information list of real card manager end includes real card information of real cards that are connected to the real card manager.

10 The simulation card is configured to receive first data sent by a transaction terminal, and to send the first data to the smart cover.

The smart cover is further configured to prompt the first data, to receive a confirming instruction for confirming that the first data is correct, and to send the first data to the real card manager.

15 The real card manager is configured to receive the first data sent by the smart cover, and to send the first data to the selected real card.

In the following, the above data interaction method or system will be described in detail. It should be understood that following embodiments can be applied in either method embodiments or system embodiments. Specifically, the data interaction method or system may include following aspects.

I. generating and updating the real card information list of real card manager end

Before the smart cover obtains the real card information list of smart cover end, the real card manager generates the real card information list of real card manager end in following manners. Certainly, the present is not limited thereto.

25 The real card manager detects the real cards that are connected to the real card manager. Specifically, the real card manager detects the contact interface and/or the contactless interface set thereon, so as to determine whether there is a real card connected to the real card manager. The real card manager may detect in turn whether there is a real card connected thereto, or the real card manager may simultaneously
30 detect whether there is a real card connected thereto. Alternatively, the real card

manager may be set to store real card information of all or part of the real cards that are connected to the real card manager, so that a user can make different settings according to security requirements of the real cards. For example, it can be set in the real card manager that obtaining real card information of some real cards is not allowed, thus
5 ensuring security of these real cards.

After detecting the real cards connected to the real card manager, the real card manager obtains the real card information of the real cards. The real card information at least includes a card number. Specifically, when detecting the real card connected thereto, the real card manager reads real card information stored in the real card
10 connected thereto. Finally, the real card manager obtains the real card information of all real cards that are connected to the real card manager. In addition, the real card information may include card authentication information and an issuer ID of the real card, in addition to the card number.

After obtaining the real card information of the real cards, the real card manager
15 generates the real card information list of real card manager end. Specifically, after obtaining the real card information of the real cards connected thereto, the real card manager generates the real card information list of real card manager end, so that the smart cover can subsequently obtain the real card information list of real card manager end, which is convenient for subsequent use. Alternatively, what the real card manager
20 can obtain is the real card information that the user sets to be allowed to be obtained.

In addition, the real card manager further generates an identification list of real card manager end in addition to the real card information list of real card manager end. Identifications in the identification list of real card manager end have a one-to-one correspondence with the real card information in the real card information list of real
25 card manager end. Specifically, each of the identifications in the identification list of real card manager end may uniquely identify a corresponding real card. Each of the identifications may be an identification that indicates whether there is a real card connected to the contact interface and/or the contactless interface (for example, 1 represents that there is a real card connected to the contact interface and/or the
30 contactless interface, and 0 represents that there is no real card connected to the contact

interface and/or the contactless interface), or each of the identifications may be one item of information such as an issuer number of a real card (for example, if the real card is a bank card, the issuer number may be a bank number), a tail number of a card number of the real card, a check value (such as a CRC check value) of a card number of the real card, or any combination thereof. The real card manager generates the identification list of real card manager end, so that it is convenient for the smart cover to update the real card information list subsequently.

Certainly, the real card manager may re-detect and generate the real card information list of real card manager end every time the real card manager is powered on. Or, the real card manager may regenerate the real card information list of real card manager end after a real card detection is triggered by a function button (a physical button or a virtual button) provided by the real card manager. Or, the real card manager may perform an operation of adding and/or deleting real card information to the real card information list every time the real card manager detects insertion or extraction of a real card, or entrance or exit of a real card.

Alternatively, the real card manager may be set to store real card information of all or part of the real cards that are connected to the real card manager, so that a user can make different settings according to security requirements of the real cards. For example, it can be set in the real card manager that obtaining real card information of some real cards is not allowed, thus ensuring security of these real cards.

Specifically, the real card manager may classify the contact interfaces and/or the contactless interfaces into a common card region and an important card region according to different usage safety factors. For example, a small account card, a secondary card, a bus card and other real cards of the user related to small amount of money are connected to interfaces in the common card region, while the large account card, a principal card of a credit card and other real cards of the user related to large amount of money are connected to interfaces in the important card region.

After classifying the contact interfaces and/or the contactless interfaces, the real card manager can read the common card region in which obtaining real card information of real cards is allowed, so as to obtain the real card information of real

cards connected to interfaces in the common card region. The real card manager can not read the important card region in which obtaining the real card information of real cards is not allowed, and thus the real card information of real cards connected to interfaces in the important card region can not be obtained. Therefore, the real card information list of real card manager end generated by the real card manager can only include the real card information of the real cards connected to interfaces in the common card region. The smart cover can obtain the real card information of the real cards connected to interfaces in the common card region rather than the real card information of the real cards connected to interfaces in the important card region. For example, the real cards connected to interfaces in the common card region are visible to the smart cover, and the smart cover can be directly connected thereto for use. The real cards connected to interfaces in the important card region are invisible to the smart cover, and the smart cover can not be directly connected thereto for use. If there is a need to connect with the real cards connected to interfaces in the important card region for use, one of following manners can be used to set the real cards connected to interfaces in the important card region, so that the smart cover can be connected to all or part of the real cards connected to interfaces in the important card region for use.

In manner 1, after the user inputs a login password, the smart cover only has an authority of connecting to and using all the real cards connected to interfaces in the common card region, but does not have an authority of connecting to and using a real card connected to interfaces in the important card region. If there is a need to connect to and use the real cards connected to interfaces in the important card region, a physical button may be set on the real card manager, or a virtual button may be set on the real card manager, or a function menu may be set on the real card manager, so that the user can set the authority of the smart cover connecting to and using the real cards connected to interfaces in the important card region on the real card manager. For example, the user may manually open the authority of the smart cover to connect to and to use all or part of the real cards connected to interfaces in the important card region by pressing the physical button, the virtual button, or an option in the function menu, and thus the smart cover can be connected to and use the real cards connected to interfaces in the important

card region whose authority is opened.

In manner 2, after the user inputs a login password, the smart cover only has an authority of connecting to and using all the real cards connected to interfaces in the common card region, and does not have an authority of connecting to and using a real card connected to interfaces in the important card region. If there is a need to connect to and use the real cards connected to interfaces in the important card region, a client may be set on the real card manager, or a control terminal (such as a PC, a smart phone, a tablet computer) connected to the real card manager may be set, and a client is set on the control terminal. The user sets the authority by logging into the client to open or close the authority of the smart cover to connect to and use all or part of the real cards connected to interfaces in the important card region, so that the smart cover can be connected to and use the real cards connected to interfaces in the important card region whose authority is opened.

In manner 3, after the user inputs a login password, the smart cover only has an authority of connecting to and using all the real cards connected to interfaces in the common card region, and does not have an authority to connect to and use a real card connected to interfaces in the important card region. If there is a need to connect to and use the real cards connected to interfaces in the important card region, a authority password may be set on the real card manager. The user can initiate a authority setting request to the real card manager through the smart cover. Only after the real card manager receives the authority setting request and the authority password input by the user, and the authority password input by the user is verified to be correct, the real card manager can open or close the authority of the smart cover to connect to and use all or part of the real cards connected to interfaces in the important card region, so that the smart cover can be connected to and use the real cards connected to interfaces in the important card region whose authority is opened. The authority password is different from the login password and an alarm password. Certainly, if the real card manager verifies that the authority password input by the user is not correct, setting the authority of connecting to and using all or part of the real cards connected to interfaces in the important card region is not executed.

II. obtaining and updating the real card information list of smart cover end

In the present disclosure, the real card information list of smart cover end obtained by the smart cover is a real card information list of real card manager end obtained from the real card manager.

5 Updating the real card information list of smart cover end may include following manners.

In manner 1, the real card manager determines whether it is required to update the real card information list of smart cover end.

10 Fig. 3 is a flow chart of a first data updating method according to an embodiment of the present disclosure. It should be understood that, the first data updating method may be realized via the data interaction method or the data interaction system. Referring to Fig. 3, the data updating method according to the present disclosure includes followings.

The smart cover searches for an identification list of smart cover end.

15 Specifically, the identification list of smart cover end is the identification list of real card manager end obtained from the real card manager by the smart cover.

If the identification list of smart cover end is found, the smart cover sends the identification list of smart cover end to the real card manager. After receiving the identification list of smart cover end sent by the smart cover, the real card manager
20 determines whether the received identification list of smart cover end is the same as the identification list of real card manager end stored in the real card manager. If they are different, the real card manager sends an updating instruction and updating data to the smart cover. After receiving the updating instruction and the updating data, the smart cover updates the real card information list of smart cover end.

25 Specifically, updating the real card information list of smart cover end may be realized as follows. The updating instruction sent by the real card manager includes an adding and/or deleting instruction, and the updating data includes real card information that needs to be added or to be deleted. After receiving the updating instruction and the updating data, the smart cover performs an adding and/or deleting operation to the real
30 card information list of smart cover end according to the updating instruction and the

updating data. Alternatively, the updating instruction sent by the real card manager includes an adding and/or deleting instruction, and the updating data includes an identification corresponding to real card information that needs to be added or to be deleted. After receiving the updating instruction and the updating data, the smart cover
5 performs an adding and/or deleting operation to the real card information list of smart cover end according to the updating instruction and the updating data. Alternatively, the updating instruction sent by the real card manager includes a replacing instruction, and the updating data includes the newest real card information list of real card manager end. After receiving the updating instruction and the updating data, the smart cover perform
10 a replacing operation to the real card information list of smart cover end according to the updating instruction and the updating data.

If the smart cover does not find the identification list of smart cover end, the smart cover sends a preset identification to the real card manager. When receiving the preset identification sent by the smart cover, and determining that the preset identification is
15 used to indicate that there is no identification list of smart cover end stored in the smart cover, the real card manager sends the updating instruction and the updating data to the smart cover. After receiving the updating instruction and the updating data, the smart cover updates the real card information list of smart cover end.

Specifically, updating the real card information list of smart cover end may be
20 realized as follows. The updating instruction sent by the real card manager includes a storing instruction, and the updating data includes the newest real card information list of real card manager end. After receiving the updating instruction and the updating data, the smart cover performs a storing operation to the real card information list of smart cover end according to the updating instruction and the updating data.

Based on the above solutions of the present disclosure, the smart cover sends the
25 identification list of smart cover end to the real card manager for determining whether the identification list of smart cover end is the same as the identification list of real card manager end, and thus data amount of data transmission is reduced, and a data transmission rate is improved, and a determining rate of the real card manager is also
30 improved, since data size of the identification list of smart cover end is much less than

that of the real card information list of smart cover end. If the smart cover is used for the first time, the smart cover itself does not store the identification list of smart cover end. At this time, the smart cover sends the preset identification to the real card manager, so that the real card manager issues the identification list of real card manager end and the
5 real card information list of real card manager end to the smart cover. The preset identification may be a null identification, a preset value, or a preset character, or the like.

Certainly, the present disclosure is not limited to the above first data updating method. When neither the smart cover nor the real card manager stores an identification
10 list, updating the real card information list of smart cover end may be realized as follows.

The real card information list of smart cover end is directly sent to the real card manager from the smart cover, so that the real card manager can determine whether or not to perform an updating after comparing the real card information list of smart cover
15 end and the real card information list of real card manager end.

Alternatively, a list number of the real card information list of smart cover end is sent to the real card manager from the smart cover, so that the real card manager can determine whether or not to perform an updating by comparing whether the list number of the real card information list of smart cover end is the same as that of the real card
20 information list of real card manager end.

Alternatively, after receiving an updating instruction input by the user, the real card manager sends the real card information list of real card manager end to the smart cover.

Certainly, after determining that an updating is required, the real card manager may send an updating inquiry request to the smart cover. The smart cover prompts the user of
25 the updating inquiry request, so that the user can determine whether or not to perform an updating.

In manner 2, the smart cover determines whether it is required to perform the updating operation for the real card information list of smart cover end.

Fig. 4 is a flow chart of a second data updating method according to an
30 embodiment of the present disclosure. It should be understood that, this second data

updating method may be realized via the data interaction method or the data interaction system. Referring to Fig. 4, the data updating method according to the present disclosure includes followings.

5 The real card manager sends the identification list of real card manager end to the smart cover.

 The smart cover receives the identification list of real card manager end sent by the real card manager, and determines whether the received identification list of real card manager end is the same as the identification list of smart cover end stored in the smart cover. Specifically, if the smart cover is used for the first time, or the smart cover never
10 successfully downloads the identification list of real card manager end, then the smart cover does not store the identification list of smart cover end, and it can be directly determined that the received identification list of real card manager end is not the same as the identification list of smart cover end stored in the smart cover.

 If the received identification list of real card manager end is not the same as the
15 identification list of smart cover end stored in the smart cover, the smart cover sends an updating request to the real card manager.

 The real card manager receives the updating request, and sends the updating instruction and the updating data to the smart cover.

 After receiving the updating instruction and the updating data sent by the real card
20 manager, the smart cover updates the real card information list of smart cover end. Specifically, updating the real card information list of smart cover end may be realized as follows. The updating instruction sent by the real card manager includes an adding and/or deleting instruction, and the updating data includes real card information that needs to be added or to be deleted. After receiving the updating instruction and the
25 updating data, the smart cover performs an adding and/or deleting operation to the real card information list of smart cover end according to the updating instruction and the updating data. Alternatively, the updating instruction sent by the real card manager includes an adding and/or deleting instruction, and the updating data includes an identification corresponding to real card information that needs to be added or to be
30 deleted. After receiving the updating instruction and the updating data, the smart cover

performs an adding and/ or deleting operation to the real card information list of smart cover end according to the updating instruction and the updating data. Alternatively, the updating instruction sent by the real card manager includes a replacing instruction, and the updating data includes the newest real card information list of real card manager end.

- 5 After receiving the updating instruction and the updating data, the smart cover perform a replacing operation to the real card information list of smart cover end according to the updating instruction and the updating data.

Based on the above solutions of the present disclosure, the real card manager sends the identification list of real card manager end to the smart cover for determining
10 whether the identification list of real card manager end is the same as the identification list of smart cover end, such that data amount of data transmission is reduced, and a data transmission rate is improved, and a determining rate of the smart cover is also improved, since data size of the identification list of real card manager end is much less than that of the real card information list of real card manager end. If the smart cover is
15 used for the first time, the smart cover itself does not store the identification list of smart cover end. At this time, after receiving the identification list of real card manager end issued by the real card manager, the smart cover directly sends the updating request, such that the real card manager can send the real card information list of real card manager end to the smart cover.

- 20 Certainly, the present disclosure is not limited to the above solution in manner 2. When neither the smart cover nor the real card manager stores an identification list, updating the real card information list of smart cover end may be realized as follows.

The real card information list of real card manager end is directly sent to the smart cover from the real card manager, so that the smart cover can directly store the real card
25 information list of real card manager end.

- Alternatively, a list number of the real card information list of real card manager end is sent to the smart cover from the real card manager, so that the smart cover can determine whether or not to perform an updating by comparing whether the list number of the real card information list of real card manager end is the same as that of the real
30 card information list of smart cover end.

Alternatively, after receiving an updating instruction input by the user, the smart cover sends the updating request to the real card manager, so that the real card manager directly issues the real card information list of real card manager end to the smart cover.

Certainly, after determining that an updating is required, the smart cover may
5 further prompt the user of determining whether or not to perform the updating, and subsequent updating operations can be executed after the user determines the updating.

The smart cover according to the present disclosure further includes a heartbeat sleep mode in addition to a normal operation mode. The heartbeat sleep mode is a non-
operating mode with low power consumption, that is, some unnecessary power
10 consumption programs are closed. Specifically, the smart cover may enter the heartbeat sleep mode when there is no operation within a preset period of time, or may be controlled to enter the heartbeat sleep mode according to an operation control of the user.

In manner 3, in the heartbeat sleep mode, the smart cover determines whether it is required to perform an updating operation for the real card information list of smart
15 cover end.

Fig. 5 is a flow chart of a third data updating method according to an embodiment of the present disclosure. It should be understood that, the third data updating method may be realized via the data interaction method or the data interaction system. Referring to Fig. 5, the data updating method according to the present disclosure includes
20 followings.

In the heartbeat sleep mode, the smart cover sends a detecting message to the real card manager every a first preset time.

The real card manager receives the detecting message, and sends a response message to the smart cover.

25 If the smart cover receives the response message in a second preset time, and the response message includes updating prompt information, the smart cover stores the updating prompt information. The updating prompt information is prompt information that the real card manager prompts the smart cover that there is an update of the real card information list of real card manager end in the real card manager.

30 After entering the operation mode from the heartbeat sleep mode, the smart cover

sends an updating triggering request to the real card manager. Specifically, the smart cover may enter the operation mode from the heartbeat sleep mode through following manners. The smart cover automatically enters the operation mode after receiving the updating prompt information. Or, the smart cover enters the operation mode after
5 receiving an operation instruction input by the user (such as an operation instruction input by the user by pressing a button).

The real card manager receives the updating triggering request, and sends the identification list of real card manager end to the smart cover.

The smart cover receives the identification list of real card manager end sent by the
10 real card manager, and determines whether the received identification list of real card manager end is the same as the identification list of smart cover end stored in the smart cover. Specifically, if the smart cover is used for the first time, or the smart cover never successfully downloads the identification list of real card manager end, then the smart cover does not store the identification list of smart cover end, and it can be directly
15 determined that the received identification list of real card manager end is not the same as the identification list of smart cover end stored in the smart cover.

If the received identification list of real card manager end is not the same as the identification list of smart cover end stored in the smart cover, the smart cover sends an updating request to the real card manager.

20 The real card manager receives the updating request, and sends the updating instruction and the updating data to the smart cover.

After receiving the updating instruction and the updating data sent by the real card manager, the smart cover updates the real card information list of smart cover end. Specifically, updating the real card information list of smart cover end may be realized
25 by following manners. The updating instruction sent by the real card manager includes an adding and/or deleting instruction, and the updating data includes real card information that needs to be added or to be deleted. After receiving the updating instruction and the updating data, the smart cover performs an adding and/or deleting operation to the real card information list of smart cover end according to the updating
30 instruction and the updating data. Or, the updating instruction sent by the real card

manager includes an adding and/or deleting instruction, and the updating data includes an identification corresponding to real card information that needs to be added or to be deleted. After receiving the updating instruction and the updating data, the smart cover performs an adding and/or deleting operation to the real card information list of smart cover end according to the updating instruction and the updating data. Or, the updating instruction sent by the real card manager includes a replacing instruction, and the updating data includes the newest real card information list of real card manager end. After receiving the updating instruction and the updating data, the smart cover perform a replacing operation to the real card information list of smart cover end according to the updating instruction and the updating data.

The first preset time may be the same as or different from the second preset time.

Based on the above solutions of the present disclosure, the real card manager sends the identification list of real card manager end to the smart cover for determining whether the identification list of real card manager end is the same as the identification list of smart cover end, such that data amount of data transmission is reduced, and a data transmission rate is improved, and a determining rate of the smart cover is also improved, since data size of the identification list of real card manager end is much less than that of the real card information list of real card manager end. If the smart cover is used for the first time, the smart cover itself does not store the identification list of smart cover end. At this time, after receiving the identification list of real card manager end issued by the real card manager, the smart cover directly sends the updating request, such that the real card manager can send the real card information list of real card manager end to the smart cover.

Certainly, the present disclosure is not limited to the above solution in manner 3. When neither the smart cover nor the real card manager stores an identification list, updating the real card information list of smart cover end may be realized by one of following manners.

The real card information list of real card manager end is directly sent to the smart cover from the real card manager, so that the smart cover can directly store the real card information list of real card manager end.

Or, a list number of the real card information list of real card manager end is sent to the smart cover from the real card manager, so that the smart cover can determine whether or not to perform an updating by comparing whether the list number of the real card information list of real card manager end is the same as that of the real card information list of smart cover end.

Or, after receiving an updating instruction input by the user, the smart cover sends the updating request to the real card manager, so that the real card manager directly issues the real card information list of real card manager end to the smart cover.

Certainly, after determining that an updating is required, the real card manager may send an updating inquiry request to the smart cover. The smart cover prompts the user of the updating inquiry request, so that the user can determine whether or not to perform the updating.

In manner 4, when the smart cover is in the heartbeat sleep mode, the real card manager determines whether it is required to perform an updating operation for the real card information list of smart cover end.

Fig. 6 is a flow chart of a fourth data updating method according to an embodiment of the present disclosure. It should be understood that, the fourth data updating method may be realized via the data interaction method or the data interaction system.

Referring to Fig. 6, a main difference between manner 4 and manner 3 is that the determining is performed by the real card manager rather than the smart cover in manner 4, which is not elaborated herein.

Alternatively, after the real card manager opens or closes the authority of the smart cover to connect to and use all or part of the real cards connected to interfaces in the important card region, since the real card information list of real card manager end is updated, the real card manager may send real card information of those real cards which the smart cover has the authority to connect to and use to the smart cover, so that the smart cover updates the real card information list of smart cover end. Or, after the real card manager opens or closes the authority of the smart cover to connect to and use all or part of the real cards connected to interfaces in the important card region, process for updating the real card information list of smart cover end is triggered, in which the

updating may be performed with reference to manner 1 and manner 2, which is not elaborated herein.

The updating data sent by the real card manager includes the identification list of real card manager end in addition to the real card information list of real card manager end, so that the smart cover can obtain a newest identification list.

III. determining the selected real card

The smart cover obtains the real card information list of smart cover end. The real card information list of smart cover end is a real card information list of real card manager end obtained from the real card manager. Alternatively, before this step, operations such as starting up the smart cover, logging into the real card manager by the smart cover may be executed, which is not elaborated herein, and reference may be made to above relative description of starting up the smart cover and logging into the real card manager by the smart cover. In this step, obtaining the real card information list of smart cover end by the smart cover may further include updating the real card information list of smart cover end by the smart cover, which is also not elaborated herein, and reference can made to above relative description of updating the real card information list of smart cover end by the smart cover. After obtaining the real card information list of real card manager end from the real card manager, the smart cover stores the real card information list of real card manager end in a storage area as the real card information list of smart cover end. When it is necessary to prompt (such as display or broadcast) the real card information list of smart cover end, the smart cover can directly obtain the real card information list of smart cover end in local, thus improving the processing speed of the smart cover.

The smart cover prompts the real card information list of smart cover end. Specifically, the smart cover displays the real card information list of smart cover end by its own displaying unit or by means of an external displaying device. Or, the smart cover plays (for example, via a loudspeaker, or via an earphone) the real card information list of smart cover end in form of voice by its own voice playing unit or by means of an external voice playing device. In this way, the user can select the real cards required for the transaction according to the real card information list of smart cover end,

thus making it convenient for the user's selection and improving the user experience.

The smart cover receives the real card selecting instruction and determines the selected real card. Specifically, the real card selecting instruction received by the smart cover may be generated by a selective physical button individually provided on the smart cover, or may be generated by a selective virtual button displayed on a touch screen of the smart cover, or may be generated by selecting a menu item representing a selection function in a menu displayed on a screen of the smart cover. The smart cover receives the real card selecting instruction and determines the selected real card. The smart cover realizes data transmission with the selected real card through the real card manager. In addition, determining the selected real card may be realized by following manners. The smart cover receives the real card selecting instruction and obtains a selected identification. The selected identification is configured to indicate the selected real card. The smart cover sends the selected identification to the real card manager. The real card manager determines the selected real card corresponding to the selected identification from the real cards that are connected to the real card manager according to the selected identification. The selected identification may be all or part of the real card information, such as the card number and/or an identification of a read-write port of the real card manager. After receiving the selected identification, the real card manager may search for an identification of a read-write port of the real card manager corresponding to the selected identification in the real card information list of real card manager end, such that the real card manager determines the read-write port thereof, thus performing data interaction with the selected real card through the determined read-write port.

IV. data interaction

The simulation card receives the first data sent by the transaction terminal, and sends the first data to the smart cover. Specifically, in the data interaction process, the simulation card and the transaction terminal (such as an ATM machine, a POS machine, a recharge machine for bus cards) are connected (through the contact interface and/or the contactless interface). The simulation card receives the first data sent by the transaction terminal. The first data may be data to be processed (such as withdrawal

amount, charge amount, real card information obtaining request).

The smart cover prompts the first data, and receives the confirming instruction for confirming that the first data is correct, and sends the first data to the real card manager. Specifically, the smart cover may display the first data, or may play (for example, via a
5 loudspeaker, or via an earphone) the first data in form of voice, so that the user can confirm whether the first data is correct. Only when the first data is correct, and the confirming instruction input by the user is received, the first data is sent to the real card manager. If the user confirms that the first data is incorrect, current data interaction may be directly cancelled. Thus, security of the data interaction is improved. The confirming
10 instruction received by the smart cover may be generated by a physical confirming button individually provided on the smart cover, or may be generated by a virtual confirming button displayed on a touch screen of the smart cover, or may be generated by selecting a confirming function in a menu displayed on a screen of the smart cover, or may be generated after a voice collecting component (such as a microphone) of the
15 smart cover receives and authenticates a voice confirming instruction, or may be generated after a fingerprint collecting component of the smart cover receives and authenticates a fingerprint confirming instruction, or may be generated after an iris collecting component of the smart cover receives and authenticates an iris confirming instruction. Certainly, the confirming instruction may be generated in any other ways,
20 which is not limited in the present disclosure.

The real card manager receives the first data sent by the smart cover, and sends the first data to the selected real card. Specifically, the real card manager sends the first data to the selected real card, so that the selected real card processes the first data. After receiving the first data, the selected real card may process the first data. The processing
25 is the same as the solution in a conventional smart card, which is not elaborated herein.

Based on the above data interaction process, various functions of different types of real cards can be realized by one simulation card. The user can complete the data interaction by just carrying the simulation card and the smart cover, without carrying real cards, thus improving convenience and security.

30 The smart cover may prompt the information that needs to be confirmed during the

data interaction process. Therefore, the interaction can be executed after the user confirms the information that needs to be confirmed during the data interaction process, thus ensuring authenticity of data interaction, and improving security.

5 In addition, since it is possible to select the real card that matches the transaction terminal for use, unnecessary costs (such as cross-bank withdrawal fees) incurred due to the fact that the user does not carry the real card matching the transaction terminal in the related art can be solved.

10 Certainly, the above specific embodiments just disclose a single data interaction from the transaction terminal to the real card. In practical application, there may be multiple data interactions, the interaction process of which is similar to the single data interaction. In the multiple data interactions, whether to prompt interactive data at the smart cover can be set according to whether it is necessary to confirm the interactive data, thus ensuring authenticity of the interactive data.

V. establishing secure connections

15 Before the smart cover obtains the real card information list of smart cover end, the present disclosure may further include a first process that a secure connection between the smart cover and the simulation card is established, and a first secure transmission key of smart cover end and a secure transmission key of simulation card end for secure data transmission between the smart cover and the simulation card are obtained.

20 Certainly, the present disclosure may further include a second process that a secure connection between the smart cover and the real card manager is established, and a second secure transmission key of smart cover end and a secure transmission key of real card manager end for secure data transmission between the smart cover and the real card manager are obtained.

25 Certainly, the above two processes may be executed at a same time, or may be executed at different times. Only one of the above two processes may be executed, or both of the above two processes may be executed.

1. A secure connection between the smart cover and the is established, and a first secure transmission key of smart cover end and a secure transmission key of simulation
30 card end for secure data transmission between the smart cover and the simulation card

are obtained.

In the present disclosure, the secure connection between the smart cover and the simulation card may be established by following manners.

In manner 1, the smart cover and the simulation card authenticate each other's identity (for example, authenticate each other's signature data). In the process of authenticating each other's identity, it is compared whether binding factors stored in the two parties are the same. After it is determined that the binding factors stored in the two parties are the same and the mutual authentication is successful, secure transmission keys (the first secure transmission key of smart cover end and the secure transmission key of simulation card end) for secure data transmission between the smart cover and the simulation card are generated.

It should be noted that, if the smart cover and the simulation card authenticate each other's certificate and identity before the secure connection between the smart cover and the simulation card is established, and a binding operation that the smart cover and the simulation card store binding factors generated in authenticating process respectively after the mutual authentication is successful, authenticating each other's identity by the smart cover and the simulation card in manner 1 is authenticating each other's identity again by the smart cover and the simulation card.

Fig. 7 is a flow chart of a first manner for establishing a secure connection between a smart cover and a simulation card according to an embodiment of the present disclosure. It should be understood that, this first manner for establishing the secure connection may be realized via the data interaction method or the data interaction system.

It can be seen that, based on the above secure connection between the smart cover and the simulation card, security of data transmission can be improved. Moreover, it can be further verified whether the smart cover is bound with the simulation card, thus further improving the security.

In addition, the present disclosure is not limited to the secure connection establishment initiated by the smart cover, and the simulation card may also be triggered by the smart cover to initiate the secure connection establishment. In this case, a first

secure connection instruction is sent to the smart cover by the simulation card, and other processes can be realized by opposite implementation subjects to the above description, which is no longer elaborated herein.

5 In manner 2, the smart cover and the simulation card authenticate each other's identity (for example, authenticate each other's signature data). Secure transmission key factors are generated in the process of authenticating each other's identity. After authenticating each other's identity, secure transmission keys (the first secure transmission key of smart cover end and the secure transmission key of simulation card end) for secure data transmission between the smart cover and the simulation card are
10 generated by using at least stored binding factors and the secure transmission key factors, and whether the secure transmission keys generated by the smart cover and the simulation card respectively are the same is verified.

It should be noted that, if the smart cover and the simulation card authenticate each other's certificate and identity before the secure connection between the smart cover and the simulation card is established, and a binding operation that the smart cover and the
15 simulation card store binding factors generated in authenticating process respectively after the mutual authentication is successful, authenticating each other's identity by the smart cover and the simulation card in manner 2 is authenticating each other's identity again by the smart cover and the simulation card.

20 Fig. 8 is a flow chart of a second manner for establishing a secure connection between a smart cover and a simulation card according to an embodiment of the present disclosure. It should be understood that, this second manner for establishing the secure connection may be realized via the data interaction method or the data interaction system.

25 In addition, the present disclosure is not limited to the secure connection establishment initiated by the smart cover, and the simulation card may also be triggered by the smart cover to initiate the secure connection establishment. In this case, a second secure connection instruction is sent to the smart cover by the simulation card, and other processes can be realized by opposite implementation subjects to the above description,
30 which is no longer described herein.

Certainly, in the process of generating the secure transmission keys for secure data transmission between the smart cover and the simulation card in above manner 1 and manner 2, the binding factors used are generated and stored by the smart cover and the simulation card in a binding process. The binding factors may be generated and stored
5 in the authenticating process after the smart cover and the simulation card authenticate each other's certificate and identity and the mutual authentication is successful. Or, the binding factors may be input manually and stored.

In addition, if there is no binding operation executed between the smart cover and the simulation card, the binding factors used in above manner 1 and manner 2 may be
10 random values manually input in the process of establishing the secure connection. Or, in the process of establishing the secure connection, the secure transmission keys are generated according to only random factors, not verifying the secure transmission keys or not using the binding factors for generating the secure transmission keys.

2. A secure connection between the smart cover and the real card manager is
15 established, and a second secure transmission key of smart cover end and a secure transmission key of real card manager end for secure data transmission between the smart cover and the real card manager are obtained.

In the present disclosure, the secure connection between the smart cover and the real card manager may be established by following manners.

20 In manner 1, the smart cover and the real card manager authenticate each other's identity. In the process of authenticating each other's identity, it is compared whether binding factors stored in the two parties are the same. After it is determined that the binding factors stored in the two parties are the same and the mutual authentication is successful, secure transmission keys (the second secure transmission key of smart cover
25 end and the secure transmission key of real card manager end) for secure data transmission between the smart cover and real card manager are generated.

It should be noted that, if a binding operation that the smart cover and the real card manager authenticate each other's certificate and identity and store binding factors generated in authenticating process respectively after the mutual authentication is
30 successful, is executed before the secure connection between the smart cover and the

real card manager is established, authenticating each other's identity by the smart cover and the real card manager in manner 1 is authenticating each other's identity again by the smart cover and the real card manager.

Differences between a solution that the smart cover and the real card manager
5 establish the secure connection through manner 1 and a solution that the smart cover and the simulation card establish the secure connection through manner 1 are as follows.

Firstly, execution subjects are different. In the solution that the smart cover and the real card manager establish the secure connection through manner 1, the execution subjects are the smart cover and the real card manager. In the solution that the smart
10 cover and the simulation card establish the secure connection through manner 1, the execution subjects are the smart cover and the simulation card. Operations that the smart cover executes are the same in the two solutions, and operations that the real card manager executes are the same as that of the simulation card.

Secondly, ways for generating secure connection instructions are different. In the
15 solution that the smart cover and the real card manager establish the secure connection through manner 1, a third secure connection instruction may be generated by a physical connection button individually provided on the smart cover, or be generated by a virtual connection button on the touch screen of the smart cover, or be generated after a power-on password is verified to be correct, or be generated when the smart cover sends a
20 login request to the real card manager, or be generated by selecting a connecting function from a menu displayed on the screen of the smart cover.

Fig. 9 is a flow chart of a first manner for establishing a secure connection between a smart cover and a real card manager according to an embodiment of the present disclosure. It should be understood that, this first manner for establishing the secure
25 connection may be realized via the data interaction method or the data interaction system.

In addition, the present disclosure is not limited to the secure connection establishment initiated by the smart cover, and the real card manager may also be triggered by the smart cover to initiate the secure connection establishment. In this case,
30 the third secure connection instruction is sent to the smart cover by the real card

manager, and other processes can be realized by opposite implementation subjects to the above description, which is no longer described herein.

In manner 2, the smart cover and real card manager authenticate each other's identity. Secure transmission key factors are generated in the process of authenticating each other's identity. After authenticating each other's identity, secure transmission keys (the second secure transmission key of smart cover end and the secure transmission key of real card manager end) for secure data transmission between the smart cover and the real card manager are generated by using at least stored binding factors and the secure transmission key factors, and it is verified whether the secure transmission keys generated by the smart cover and the real card manager are the same.

It should be noted that, if a binding operation that, the smart cover and the real card manager authenticate each other's certificate and identity store binding factors generated in authenticating process respectively after the mutual authentication is successful, is executed before the secure connection between the smart cover and the real card manager is established, authenticating each other's identity by the smart cover and the real card manager in manner 2 is authenticating each other's identity again by the smart cover and the real card manager.

Differences between a solution that the smart cover and the real card manager establish the secure connection through manner 2 and a solution that the smart cover and the simulation card establish the secure connection through manner 2 are as follows.

Firstly, execution subjects are different. In the solution that the smart cover and the real card manager establish the secure connection through manner 2, the execution subjects are the smart cover and the real card manager. In the solution that the smart cover and the simulation card establish the secure connection through manner 2, the execution subjects are the smart cover and the simulation card. Operations that the smart cover executes are the same in the two solutions, and operations that the real card manager executes are the same as that of the simulation card.

Secondly, ways for generating secure connection instructions are different. In the solution that the smart cover and the real card manager establish the secure connection through manner 2, a fourth secure connection instruction may be generated by a

physical connection button individually provided on the smart cover, or be generated by a virtual connection button on the touch screen of the smart cover, or be generated after that a power-on password is verified to be correct, or be generated when the smart cover sends a login request to the real card manager, or be generated by selecting a connecting
5 function from a menu displayed on the screen of the smart cover.

Fig. 10 is a flow chart of a second manner for establishing a secure connection between a smart cover and a real card manager according to an embodiment of the present disclosure. It should be understood that, this second manner for establishing the secure connection may be realized via the data interaction method or the data interaction
10 system.

In addition, the present disclosure is not limited to the secure connection establishment initiated by the smart cover, and the real card manager may also be triggered by the smart cover to initiate the secure connection establishment. In this case, a fourth secure connection instruction is sent to the smart cover by the real card manager,
15 and other processes can be realized by opposite implementation subjects to the above description, which is no longer described herein.

Certainly, in the process of generating the secure transmission keys for secure data transmission between the smart cover and the real card manager in above manner 1 and manner 2, the binding factors used are generated and stored by the smart cover and the
20 real card manager in a binding process. The binding factors may be generated and stored in the authenticating process after the smart cover and the real card manager authenticate the each other's certificate and identity and the mutual authentication is successful. Or, the binding factors may be input manually and stored.

In addition, if there is no binding operation executed between the smart cover and
25 the real card manager, the binding factors used in above manner 1 and manner 2 may be random values manually input in the process of establishing the secure connection. Or, in the process of establishing the secure connection, the secure transmission keys are generated according to only random factors, not verifying the secure transmission keys or not using the binding factors for generating the secure transmission keys.

30 In addition, in the present disclosure, before the secure connection between the

smart cover and the real card manager is established, and the second secure transmission key of smart cover end and the secure transmission key of real card manager end for secure data transmission between the smart cover and the real card manager are obtained, the smart cover sends a login request to the real card manager. Specifically, the login request may be generated by a physical login button individually provided on the smart cover, or be generated by a virtual login button on the touch screen of the smart cover, or be generated after a power-on password is verified to be correct, or be generated by selecting a login function from a menu displayed on the screen of the smart cover. The login request may include a unique identifier of the smart cover, such that the real card manager knows which smart cover requests to login.

After the smart cover sends the login request to the real card manager, the secure connection between the smart cover and the real card manager is established, and the second secure transmission key of smart cover end and the secure transmission key of real card manager end for secured data transmission between the smart cover and the real card manager are obtained, following operations are executed.

The smart cover performs a first processing to a received login password with the second secure transmission key of smart cover end, and sends the first processed login password to the real card manager. Specifically, the smart cover may further prompt the user of inputting the login password. After the user inputs a login password, the smart cover performs the first processing to the login password with the second secure transmission key of smart cover end, and sends the first processed login password to the real card manager, thus improving security of login password transmission.

The real card manager receives the data sent by the smart cover, performs a second processing to the received data with the secure transmission key of real card manager end, and verifies accuracy of the second processed data. Specifically, after performing the second processing to the data sent by the smart cover with the secure transmission key of real card manager end, the real card manager obtains the login password input by the user, and compares the login password with a stored legal login password. Only if the login password input by the user is the same as the stored legal login password, the smart cover is allowed to log in the real card manager, thus improving login security,

and ensuring security of subsequent data transmission. If the real card manager according to the present disclosure has an alarming function, a legal login password and an alarm password may be preset in the real card manager. In this case, the real card manager obtains a password to be verified after performing the second processing to the received data with the secure transmission key of real card manager end. The real card manager judges whether the password to be verified is the alarm password. If the password to be verified is not the alarm password and is the login password, the real card manager determines that the password to be verified passes the verification. Since the alarm password is set, the real card manger can recognize that there is a security risk in current login, and performs the alarming operation (for example, the real card manger sends an alarming message, or dials an alarming call to law enforcement, or the like) when the login password input by the user is the alarm password.

After the real card manager verifies that the second processed data passes the verification, the smart cover logs in the real card manager.

It can be seen that, before the secure connection between the smart cover and the real card manager is established, the smart cover sends the login request, and the secure connection establishment is triggered while the smart cover sends the login request. After the secure connection is established, the login password is verified, thus saving process and improving processing speed.

In addition, in order to ensure effectiveness of the real card information list of smart cover end, the real card information list of smart cover end may be updated by following manners after the secure connection between the smart cover and the real card manger is established and the smart cover logs in the real card manager,.

In manner 1, after the smart cover logs in the real card manager, the real card manager judges whether it is required to perform operations for updating the real card information list of smart cover end.

Referring to previous description, manner 1 is different from the previous description in that: after establishing the secure connection, when sending data, the smart cover and the real card manager perform the first processing to the data to be sent with transmission keys. Accordingly, when receiving the data, the smart cover and the

real card manager may first perform the second processing to the received data with the transmission keys, and then perform subsequent processing. It is no longer described herein.

5 In manner 2, after the smart cover logs in the real card manager, the smart cover judges whether it is required to perform operations for updating the real card information list of smart cover end.

Referring to previous description, what is different from the previous description is that: after establishing the secure connection, when sending data, the smart cover and the real card manager perform the first processing to the data to be sent with transmission keys. Accordingly, when receiving the data, the smart cover and the real card manager may first perform the second processing to the received data with the transmission keys, and then perform subsequent processing. It is no longer described herein.

15 The smart cover according to the present disclosure further includes a heartbeat sleep mode in addition to a normal operation mode. The heartbeat sleep mode is a non-operating mode with low power consumption, that is, some unnecessary power consumption programs are closed. Specifically, the smart cover may enter the heartbeat sleep mode if there is no operation within a preset period of time, or be controlled to enter the heartbeat sleep mode according to operation of the user.

20 In the heartbeat sleep mode, the smart cover may further judge whether or not to maintain the secure connection established between the smart cover and the real card manager, so that when the smart cover recovers to the operation mode from the heartbeat sleep mode, the smart cover does not need to establish the secure connection with the real card manager again, thus improving convenience.

25 A specific implementation for the smart cover to judge whether or not to maintain the secure connection established between the smart cover and the real card manager in the heartbeat sleep mode is provided in the following.

In the heartbeat sleep mode, the smart cover sends a detecting message to the real card manager every a first preset time.

30 The real card manager receives the detecting message, and sends a response

message to the smart cover.

If the smart cover does not receive the response message in a second preset time, the smart cover breaks the secure connection between the smart cover and the real card manager.

5 If the smart cover receives the response message in a second preset time, the smart cover maintains the established secure connection between the smart cover and the real card manager.

10 If the smart cover does not receive the response message in the second preset time, network between the smart cover and the real card manager may be unstable, or the real card manger may work abnormally, and thus, in this case, by breaking the secure connection between the smart cover and the real card manager, security may be ensured. If the smart cover receives the response message in the second preset time, the smart cover maintains the secure connection between the smart cover and the real card manager, such that the smart cover does not need to establish the secure connection again when the smart cover recovers to the operation mode, thus making it convenient to use.

15 Certainly, in the heartbeat sleep mode, the user can also choose to manually break the secure connection between the smart cover and the real card manager, for example, by an operation that makes the smart cover log out of the real card manager, or a shutdown operation performed by the user to the smart cover.

20 The first preset time may be the same as or different from the second preset time.

Manners for updating the real card information list of smart cover end in the heartbeat sleep mode are provided in the following.

25 In manner 3, after the smart cover logs in the real card manager, the smart cover is in the heartbeat sleep mode, and the smart cover judges whether there is a need to perform operations for updating the real card information list of smart cover end.

30 In the heartbeat sleep mode, that the smart cover judges whether there is a need to perform operations for updating the real card information list of smart cover end may refer to previous description, what is different from the previous description is that: after establishing the secure connection, when sending data, the smart cover and the real card

manager perform the first processing to the data to be sent with transmission keys. Accordingly, when receiving the data, the smart cover and the real card manager may first perform the second processing to the received data with the transmission keys, and then perform subsequent processing. It is no longer described herein.

5 In manner 4, after the smart cover logs in the real card manager, the smart cover is in the heartbeat sleep mode, and the real card manager judges whether it is necessary to perform operations for updating the real card information list of smart cover end.

10 In the heartbeat sleep mode, that the real card manager judges whether it is necessary to perform operations for updating the real card information list of smart cover end may refer to previous description, what is different from the previous description is that: after establishing the secure connection, when sending data, the smart cover and the real card manager perform the first processing to the data to be sent with transmission keys. Accordingly, when receiving the data, the smart cover and the real card manager may first perform the second processing to the received data with the transmission keys, and then perform subsequent processing. It is no longer described herein.

VI. binding

20 In order to further improve the security of data interaction, before establishing the secure connection between the smart cover and the simulation card, a process of performing a binding operation to the smart cover and the simulation card may further be included.

Before establishing the secure connection between the smart cover and the real card manager, the process of performing a binding operation to the smart cover and the real card manager may further be included.

25 Certainly, the above two processes may be executed at the same time, or may be executed at different times. Only one of the above two processes may be executed, or both of the above two processes may be executed.

1. The smart cover and the simulation card perform the binding operation.

30 In the present disclosure, the smart cover and the simulation card may be bound by following manners.

The smart cover and the simulation card authenticate each other's certificate and identity, and store the binding factors generated in authenticating process after the mutual authentication is successful.

Fig. 11 is a flow chart of performing a binding operation between a smart cover and a simulation card according to an embodiment of the present disclosure. It should be understood that, the binding operation may be realized via the data interaction method or the data interaction system.

It can be seen that, based on the above operation for binding the smart cover and the simulation card, the security of subsequent data interaction between the smart cover and the simulation card can be ensured.

In addition, the above operation for binding the smart cover and the simulation card is not necessary. It is possible to select performing or not performing the above operation for binding the smart cover and the simulation card according to needs of different application scenarios.

Certainly, the operation for binding the smart cover and the simulation card is not limited to the above implementation. For example, manual binding can also be used. That is, in a credible environment, an identification of a simulation card to be bound is input on the smart cover as a first binding factor of smart cover end, and the identification of the simulation card is taken as a default binding factor of simulation card end by the simulation card. Or, a contact connection is performed between the smart cover and the simulation card, and a random value is input on the smart cover as the first binding factor of smart cover end, and the input random value is sent by the smart cover to the simulation card through the contact connection, as the binding factor of simulation card end. Any other implementation that can make the smart cover and the simulation card obtain the same binding factors should belong to the scope of the present disclosure.

2. The smart cover and the real card manager performs binding operation.

In the present disclosure, the smart cover and the real card manager may be bound by following manners.

The smart cover and the real card manager authenticate each other's certificate and

identity, and store binding factors generated in authenticating process after the mutual authentication is successful.

Fig. 12 is a flow chart of performing a binding operation by a smart cover and a real card manager according to an embodiment of the present disclosure. It should be understood that, the binding operation may be realized via the data interaction method
5 or the data interaction system.

Certainly, it is not necessary to perform the above operation for binding the smart cover and the simulation card and the above operation for binding the smart cover and the real card manager at the same time. According to needs of different application scenarios, it is possible to select performing only the operation for binding the smart
10 cover and the simulation card, or performing only the operation for binding the smart cover and the real card manager, or performing neither one.

VII. data interaction.

After the secure connection is established between the smart cover and the simulation card, a first processing is performed on the first data sent by the simulation
15 card to the smart cover using the secure transmission key of simulation card end, and then the first data after the first processing is sent to the smart cover. After receiving the first data obtained after the first processing, the smart cover performs a second processing using the first secure transmission key of smart cover end.

After the secure connection between the smart cover and the real card manager is established, the first data is sent by the smart cover to the real card manger after a first
20 processing is performed on the first data using the second secure transmission key of smart cover end. After receiving the first data obtained after the first processing, the real card manager performs a second processing with the secure transmission key of real card manager end.
25

Thus, the security of data interaction is ensured.

In the following, a data interaction method after establishing a secure connection between the smart cover and the simulation card and establishing a secure connection between the smart cover and the real card manager of the present disclosure is
30 provided, but the present disclosure is not limited thereto.

The simulation card receives data sent by the transaction terminal, and sends the data to the smart cover after performing the first processing on the received data with the secure transmission key of simulation card end. Specifically, in the data interaction process, the simulation card and the transaction terminal (such as an ATM machine, a POS machine, a recharge machine for bus cards) are connected (through the contact interface and/or the contactless interface). The simulation card receives the data sent by the transaction terminal, and the data may be data to be processed (such as withdrawal amount, charge amount, real card information obtaining request).

After the smart cover receives data sent by the simulation card, and performs the second processing on the received data with the first secure transmission key of smart cover end, and after the smart cover receives a confirming instruction for confirming that the data obtained after the second processing is correct, the smart cover uses the second secure transmission key of smart cover end to perform the first processing on the data obtained after the second processing and sends the data obtained after the first processing to the real card manager. Specifically, after receiving the data sent by the simulation card, and performing the second processing on the received data with the first secure transmission key of smart cover end, the smart cover may further display the data to be processed, or may play (for example, play by a loudspeaker, or play by an earphone) the data to be processed, so that the user can confirm whether the data to be processed is correct. Only when the data to be processed is correct, and the confirming instruction for confirming that the data to be processed is correct input by the user is received, the data to be processed is sent to the real card manager. If the user confirms that the data to be processed is incorrect, current data interaction may be directly cancelled. Thus, security of the data interaction is improved. The confirming instruction received by the smart cover for confirming that the data obtained after the second processing is correct may be generated by a physical confirming button individually provided on the smart cover, or may be generated by a virtual confirming button displayed on a touch screen of the smart cover, or may be generated by selecting a confirming function from a menu displayed on a screen of the smart cover, or may be generated after a voice collecting component (such as a microphone) of the smart cover

receives and authenticates a voice confirming instruction, or may be generated after a fingerprint collecting component of the smart cover receives and authenticates a fingerprint confirming instruction, or may be generated after an iris collecting component of the smart cover receives and authenticates an iris confirming instruction.

5 Certainly, the confirming instruction may be generated in any other ways, which is not limited in the present disclosure.

The real card manager receives data sent by the smart cover, and sends the data to the selected real card after performing the second processing on the received data with the secure transmission key of real card manager end. Specifically, the real card
10 manager sends the data to be processed to the selected real card, such that the selected real card processes the data to be processed.

Based on the above the data interaction process, various functions of different types of real cards can be realized by one simulation card. The user can complete the data interaction by just carrying the simulation card and the smart cover, without
15 carrying real cards, thus improving convenience and security.

The smart cover may prompt information that needs to be confirmed during the data interaction process, and therefore, the user can perform the data interaction after confirming the information that needs to be confirmed during the data interaction process, thus ensuring authenticity of data interaction, and improving security.

20 In the data transmission process, encryption and decryption operations and/or verification operations are performed during data interactions among the simulation card, the smart cover and the real card manager, thus ensuring security and integrity of data transmission.

In addition, since it is possible to select and use the real card that matches the transaction terminal, unnecessary costs (such as cross-bank withdrawal fees) incurred
25 due to the fact that the user does not carry the real card matching the transaction terminal in the related art can be solved.

VIII. recharging

With the data interaction architecture according to the present disclosure,
30 recharging operations (such as recharging for bus cards, water cards and electric cards,

etc.) may be realized. Thus, it is convenient for the user to realize recharging for different types of real cards just by carrying the simulation card and the smart cover, which is convenient to carry, thus avoiding property damage due to losing the real cards.

In the following, a specific flow for recharging is provided, but the present is not
5 limited thereto.

The smart cover obtains the real card information list of smart cover end. The real card information list of smart cover end is a real card information list of real card manager end obtained from the real card manager. Alternatively, before this step, operations such as starting up the smart cover, logging into the real card manager by the
10 smart cover may be executed, which is no longer described herein, and reference can be made to above relative description of starting up the smart cover and logging into the real card manager by the smart cover. In this step, obtaining the real card information list of smart cover end by the smart cover may further include a step of updating the real card information list of smart cover end by the smart cover, which is no longer
15 described herein, and reference can be made to above relative description of updating the real card information list of smart cover end by the smart cover. After obtaining the real card information list of real card manager end from the real card manager, the smart cover stores the real card information list of real card manager end in a storage area as the real card information list of smart cover end. When it is necessary to prompt (such
20 as display or voice play) the real card information list of smart cover end, the smart cover can obtain the real card information list of smart cover end in local, thus improving processing speed of the smart cover.

The smart cover prompts the real card information list of smart cover end. Specifically, the smart cover displays the real card information list of smart cover end
25 by its own displaying device or by means of an external displaying device. Or, the smart cover plays (for example, plays by a loudspeaker, or plays by an earphone) the real card information list of smart cover end in form of voice by its own voice playing device or by means of an external playing device. In this way, the user selects the real card to be used for recharging according to the real card information list of smart cover end, which
30 makes it convenient for the user's selection, thus improving the user experience.

The smart cover receives the real card selecting instruction and determines the selected real card. The simulation card receives data sent by a recharging terminal, and performs the first processing on the received data with the secure transmission key of simulation card end, and sends the data obtained after first processing to the smart cover.

5 Specifically, the real card selecting instruction received by the smart cover may be generated by a physical selection button individually provided on the smart cover, or may be generated by a virtual selection button displayed on a touch screen of the smart cover, or may be generated by selecting a menu item representing a selection function from a menu displayed on a screen of the smart cover. The smart cover receives the real

10 card selecting instruction and determines the selected real card. The smart cover realizes data transmission with the selected real card through the real card manager. In addition, in the recharging process, the simulation card and the recharging terminal (such as recharging machine) are connected (through the contact interface or the contactless interface). The simulation card receives the data sent by the recharging terminal, in

15 which the data may be recharging data to be processed (such as recharging amount), such that the user can subsequently confirm whether the recharging data to be processed is correct. In addition, before receiving the recharging data to be processed sent by the recharging terminal, the simulation card may further receive a request for obtaining real card information of the selected real card sent by the recharging terminal. The smart

20 cover receives data sent by the simulation card, and performs the second processing on the received data with the first secure transmission key of smart cover end, and then performs the first processing on the data obtained after the second processing with the second secure transmission key of smart cover end, and sends the data obtained after the first processing to the real card manager. The real card manager receives the data sent

25 by the smart cover, and performs the second processing on the received data with the secure transmission key of real card manager end, and then sends the data obtained after the second processing to the selected real card. The selected real card receives the data sent by the real card manager, and then sends the obtained real card information to the real card manager. The real card manager receives the data sent by the selected real card,

30 and performs the first processing on the received data with the secure transmission key

of real card manager end, and then sends the data obtained after the first processing to the smart cover. The smart cover receives the data sent by the real card manager, and performs the second processing on the received data with the second secure transmission key of smart cover end, and then performs the first processing with the first secure transmission of smart cover end on the data obtained after the second processing, and sends the data obtained after the first processing to the simulation card. The simulation card receives the data sent by the smart cover, and performs the second processing on the received data with the secure transmission key of simulation card end, then sends the data obtained after the second processing to the recharging terminal. Thus the recharging terminal obtains the real card information of the selected real card, which is convenient to recharge the real card subsequently.

The smart cover receives the data sent from the simulation card, and performs the second processing on the received data with the first secure transmission key of smart cover end, and then prompts the data obtained after the second processing. After receiving the confirming instruction for confirming that the data obtained after the second processing is correct, the smart cover performs the first processing with the second secure transmission key of smart cover end on the data obtained after the second processing, and then sends the data obtained after the first processing to the real card manager. Specifically, the smart cover may display the recharging data to be processed, or voice play (for example, play by a loudspeaker, or play by an earphone) the recharging data to be processed, so that the user can confirm whether the recharging data to be processed is correct. Only when the recharging data to be processed is correct, and the confirming instruction input by the user for confirming that the recharging data to be processed is correct is received, the recharging data to be processed is sent to the real card manager. If the user confirms that the recharging data to be processed is incorrect, current recharging may be directly cancelled. Thus, security of recharging is improved. The confirming instruction received by the smart cover for confirming that the data obtained after the second processing is correct may be generated by a physical confirming button individually provided on the smart cover, or may be generated by a virtual confirming button displayed on a touch screen of the smart cover, or may be

generated by selecting a confirming function from a menu displayed on a screen of the smart cover, or may be generated after a voice collecting component (such as a microphone) of the smart cover receives and authenticates a voice confirming instruction, or may be generated after a fingerprint collecting component of the smart cover receives and authenticates a fingerprint confirming instruction, or may be generated after an iris collecting component of the smart cover receives and authenticates an iris confirming instruction. Certainly, the confirming instruction may be generated in any other ways, which is not limited in the present disclosure.

The real card manager receives data sent by the smart cover, performs the second processing on the received data with the secure transmission key of real card manager end, and then sends the data obtained after the second processing to selected real card. Specifically, the real card manager sends the recharging data to be processed to the selected real card, such that the selected real card processes the recharging data to be processed (such as performing recharging operation).

Based on the above recharging process, various functions of different types of real cards can be realized by one simulation card. For recharging, the user can just carries the simulation card and the smart cover, without carrying real cards, thus improving convenience and security of recharging.

The smart cover may prompt information that needs to be confirmed during the recharging process, and therefore the user can perform recharging after confirming the information that needs to be confirmed during the recharging process, thus ensuring authenticity of recharging, and improving security.

In the data transmission process, encryption and decryption operations and/or verification operations are performed during data interactions among the simulation card, the smart cover and the real card manager, thus ensuring security and integrity of data transmission.

In addition, since it is possible to select and use the real card that matches the recharging terminal, unnecessary costs (such as cross-bank withdrawal fees) incurred due to the fact that the user does not carry the real card matching the recharging terminal in the related art can be solved.

IX. transaction

With the data interaction architecture according to the present disclosure, transaction operations (such as withdrawing or transferring at an ATM, or charging on the POS machine) can also be realized. Thus, it is convenient for the user to realize transaction of different types of real cards just by carrying the simulation card and the smart cover, which is convenient for the user's carrying, thus avoiding property damage due to losing the real cards.

In the following, a specific flow for transaction is provided, but the present is not limited thereto.

10 The smart cover obtains the real card information list of smart cover end. The real card information list of smart cover end is a real card information list of real card manager end obtained from the real card manager. Alternatively, before this step, operations such as starting up the smart cover, logging into the real card manager by the smart cover may be executed, which is no longer described herein, and reference can be made to above relative description of starting up the smart cover and logging into the real card manager by the smart cover. In this step, obtaining the real card information list of smart cover end by the smart cover may further include a step of updating the real card information list of smart cover end by the smart cover, which is no longer described herein, and reference can be made to above relative description of updating the real card information list of smart cover end by the smart cover. After obtaining the real card information list of real card manager end from the real card manager, the smart cover stores the real card information list of real card manager end in a storage area thereof as the real card information list of smart cover end. When it is necessary to prompt (such as display or voice play) the real card information list of smart cover end, 20 the smart cover can directly obtain the real card information list of smart cover end in local, thus improving processing speed of the smart cover.

 The smart cover prompts the real card information list of smart cover end. Specifically, the smart cover displays the real card information list of smart cover end by its own displaying device or by means of an external displaying device. Or, the smart cover plays (for example, plays by a loudspeaker, or plays by an earphone) the real card 30

information list of smart cover end in form of voice by its own voice playing device or by means of an external playing device. In this way, the user can select the real card to be used for the transaction according to the real card information list of smart cover end, which makes it convenient for the user's selection, thus improving the user experience.

5 The smart cover receives the real card selecting instruction and determines the selected real card. The simulation card receives data sent by a transaction terminal, and performs the first processing on the received data with the secure transmission key of simulation card end, and sends the data obtained after the first processing to the smart cover. Specifically, the real card selecting instruction received by the smart cover may
10 be generated by a physical selection button individually provided on the smart cover, or may be generated by a virtual selection button displayed on a touch screen of the smart cover, or may be generated by selecting a menu item representing a selection function from a menu displayed on a screen of the smart cover. The smart cover receives the real card selecting instruction and determines the selected real card. The smart cover realizes
15 data transmission with the selected real card through the real card manager. In addition, in the transaction process, the simulation card and the transaction terminal (such as an ATM machine or a POS machine) are connected (through the contact interface or the contactless interface). The simulation card receives the data sent by the transaction terminal, in which the data may be transaction data to be processed (such as withdrawal
20 amount, charge amount), such that the user can subsequently confirm whether the transaction data to be processed is correct. In addition, before receiving the transaction data to be processed sent by the transaction terminal, the simulation card may further receive a request sent by the transaction terminal for obtaining real card information of the selected real card. The smart cover receives data sent by the simulation card, and
25 performs the second processing on the received data with the first secure transmission key of smart cover end, and then performs the first processing with the second secure transmission key of smart cover end on the data obtained after the second processing, and sends the data obtained after the first processing to the real card manager. The real card manager receives the data sent by the smart cover, and performs the second
30 processing on the received data with the secure transmission key of real card manager

end, and then sends the data obtained after the second processing to the selected real card. The selected real card receives the data sent by the real card manager, and then sends the obtained real card information to the real card manager. The real card manager receives the data sent by the selected real card, and performs the first processing on the received data with the secure transmission key of real card manager end, and then sends
5 the data obtained after the first processing to the smart cover. The smart cover receives the data sent by the real card manager, and performs the second processing on the received data with the second secure transmission key of smart cover end, and then performs the first processing with the first secure transmission of smart cover end on the data obtained after the second processing, and sends the data obtained after the first
10 processing to the simulation card. The simulation card receives the data sent by the smart cover, and performs the second processing to the received data with the secure transmission key of simulation card end, and then sends the data obtained after the second processing to the transaction terminal. Thus, the transaction terminal obtains the real card information of the selected real card, which is convenient for subsequent
15 transaction with respect to the real card.

The smart cover receives the data sent from the simulation card, and performs the second processing on the received data with the first secure transmission key of smart cover end, and then prompts the data obtained after the second processing. After
20 receiving the confirming instruction for confirming that the data obtained after the second processing is correct, the smart cover performs the first processing with the second secure transmission key of smart cover end on the data obtained after the second processing, and then sends the data obtained after the first processing to the real card manager. Specifically, the smart cover may display the transaction data to be processed, or voice play (for example, play by a loudspeaker, or play by an earphone) the
25 transaction data to be processed, so that the user can confirm whether the transaction data to be processed is correct. Only when the transaction data to be processed is correct, and the confirming instruction input by the user for confirming that the transaction data to be processed is correct is received, the transaction data to be processed is sent to the
30 real card manager. If the user confirms that the transaction data to be processed is

incorrect, current transaction may be directly cancelled. Thus, security of transaction is improved. The confirming instruction received by the smart cover for confirming that the data obtained after the second processing is correct may be generated by a physical confirming button individually provided on the smart cover, or may be generated by a virtual confirming button displayed on a touch screen of the smart cover, or may be generated by selecting a confirming function from a menu displayed on a screen of the smart cover, or may be generated after a voice collecting component (such as a microphone) of the smart cover receives and authenticates a voice confirming instruction, or may be generated after a fingerprint collecting component of the smart cover receives and authenticates a fingerprint confirming instruction, or may be generated after an iris collecting component of the smart cover receives and authenticates an iris confirming instruction. Certainly, the confirming instruction may be generated in any other ways, which is not limited in the present disclosure.

The real card manager receives data sent by the smart cover, performs the second processing on the received data with the secure transmission key of real card manager end, and then sends the data obtained after the second processing to selected real card. Specifically, the real card manager sends the transaction data to be processed to the selected real card, such that the selected real card processes the transaction data to be processed.

The selected real card receives the data sent by the real card manager, performs the transaction processing, and sends the data obtained after the transaction processing to the real card manager. Specifically, the selected real card performs transaction processing on the transaction data to be processed, in which the transaction processing is a conventional solution of transaction processing in the related art, which is no longer described herein.

The real card manager receives the data sent by the selected real card, and performs the first processing on the received data with the secure transmission key of real card manager end, and then sends the data obtained after the first processing to the smart cover.

The smart cover receives the data sent by the real card manager, and performs the

second processing on the received data with the second secure transmission key of smart cover end, and then performs the first processing with the first secure transmission key of smart cover end on the data obtained after the second processing, and sends the data obtained after the first processing to the simulation card.

5 The simulation card receives the data sent by the smart cover, and performs the second processing on the received data with the secure transmission key of simulation card end, and then sends the data obtained after the second processing to the transaction terminal. Specifically, after receiving the data obtained after transaction processing performed by the selected real card, the transaction terminal can complete current
10 transaction, such as withdrawing money, transferring, deducting money by charging, according to existing transaction flow.

 Based on the above transaction process, various functions of different types of real cards can be realized by one simulation card. For transaction, the user can just carries the simulation card and the smart cover, without carrying real cards, thus improving
15 convenience and security of transaction.

 The smart cover may prompt information that needs to be confirmed during the transaction process, and therefore the user can perform transaction after confirming the information that needs to be confirmed during the transaction process, thus ensuring authenticity of transaction, and improving security.

20 In the data transmission process, encryption and decryption operations and/or verification operations are performed during data interactions among the simulation card, the smart cover and the real card manager, thus ensuring security and integrity of data transmission.

 In addition, since it is possible to select real card that matches the transaction
25 terminal for use, unnecessary costs (such as cross-bank withdrawal fees) incurred due to the fact that the user does not carry the real card matching the transaction terminal in the related art can be solved.

 Certainly, the above specific embodiment just discloses a single data interaction from the transaction terminal to the real card and from the real card to the transaction
30 terminal. In practical application, there may be multiple data interactions, interaction

process of which is similar to the single data interaction. In the multiple data interactions, whether to prompt interactive data at the smart cover can be set according to whether it is necessary to confirm interactive data, thus ensuring authenticity of the interactive data.

5 X. updating application

1. Updating the application of the smart cover.

In the present disclosure, the smart cover can update its own installed applications or install a new application, so as to extend various applications of the smart cover or to update existing applications of the smart cover.

10 A specific implementation for updating the application of the smart cover is provided in the present disclosure, but the present disclosure is not limited thereto.

Fig. 13 is a flow chart of updating an application of a smart cover according to an embodiment of the present disclosure. It should be understood that, the updating process may be realized via the data interaction method or the data interaction system.

15 Based on updating the application of the smart cover in the present disclosure, not only the installed application can be updated, but also the new application can be downloaded and installed, thus extending functions of the smart cover, and making it convenient for the user to use the smart cover.

2. Updating the application of the simulation card.

20 In the present disclosure, the simulation card can update installed applications of its own or install a new application, so as to extend various applications of the simulation card or to update existing applications of the simulation card.

A specific implementation for updating the application of the simulation card is provided in the present disclosure, but the present disclosure is not limited thereto.

25 Fig. 14 is a flow chart of updating an application of a simulation card according to an embodiment of the present disclosure. It should be understood that, the updating process may be realized via the data interaction method or the data interaction system.

Based on updating the application of the simulation card in the present disclosure, not only the installed application can be updated, but also the new application can be
30 downloaded and installed, thus extending functions of the simulation card, and making

it convenient for the user to use the simulation card.

Certainly, if the secure connection between the smart cover and the simulation card is not established, the simulation card directly sends the data to the smart cover, and the smart cover directly sends the data to the simulation card, when the simulation card
5 performs the application updating.

3. Updating the application of the real card manager.

In the present disclosure, the real card manager can update installed applications of its own or install a new application, so as to extend various applications of the real card manager or to update existing applications of the real card manager.

10 A specific implementation for updating the application of the real card manager is provided in the present disclosure, but the present disclosure is not limited thereto.

Fig. 15 is a flow chart of updating an application of a real card manager according to an embodiment of the present disclosure. It should be understood that, the updating process may be realized via the data interaction method or the data interaction system.

15 Based on updating the application of the real card manager in the present disclosure, not only the installed application can be updated, but also the new application can be downloaded and installed, thus extending functions of the real card manager, and making it convenient for the user's usage.

In embodiments of the present disclosure, for all the normal data interaction
20 process between the smart cover and the simulation card, the simulation card is in an effective communication range of the smart cover. If the smart cover detects that the simulation card is out of the effective communication range of the smart cover, the smart cover may prompt the user, or sends a prompt message to a user terminal (such as a smart phone, a tablet computer, etc.), so as to prompt the user of abnormal position of
25 the simulation card, thus improving security for using the simulation card.

Any process or method described in a flow chart or described herein in other ways may be understood to include one or more modules, segments or portions of codes of executable instructions for achieving specific logical functions or steps in the process, and the scope of a preferred embodiment of the present disclosure includes other
30 implementations, in which the order of execution is different from that which is

depicted or discussed, including executing functions in a substantially simultaneous manner or in an opposite order according to the related functions. This should be understood by those skilled in the art to which embodiments of the present disclosure belong.

5 It should be understood that each part of the present disclosure may be realized by the hardware, software, firmware or their combination. In the above embodiments, multiple steps or methods may be realized by the software or firmware stored in the memory and executed by the appropriate instruction execution system. For example, if it is realized by the hardware, likewise in another embodiment, the steps or methods
10 may be realized by one or a combination of the following techniques known in the art: a discrete logic circuit having a logic gate circuit for realizing a logic function of a data signal, an application-specific integrated circuit having an appropriate combination logic gate circuit, a programmable gate array (PGA), a field programmable gate array (FPGA), etc.

15 Those skilled in the art shall understand that all or parts of the steps in the above exemplifying method of the present disclosure may be achieved by commanding the related hardware with programs. The programs may be stored in a computer readable storage medium, and the programs comprise one or a combination of the steps in the method embodiments of the present disclosure when run on a computer.

20 In addition, each function cell of the embodiments of the present disclosure may be integrated in a processing module, or these cells may be separate physical existence, or two or more cells are integrated in a processing module. The integrated module may be realized in a form of hardware or in a form of software function modules. When the integrated module is realized in a form of software function module and is sold or used
25 as a standalone product, the integrated module may be stored in a computer readable storage medium.

 The storage medium mentioned above may be read-only memories, magnetic disks, CD, etc.

 Reference throughout this specification to “an embodiment,” “some
30 embodiments,” “an example,” “a specific example,” or “some examples,” means

that a particular feature, structure, material, or characteristic described in connection with the embodiment or example is included in at least one embodiment or example of the present disclosure. The appearances of the phrases throughout this specification are not necessarily referring to the same embodiment or example of the present disclosure. Furthermore, the particular features, structures, materials, or characteristics may be combined in any suitable manner in one or more embodiments or examples.

Although explanatory embodiments have been shown and described, it would be appreciated by those skilled in the art that the above embodiments cannot be construed to limit the present disclosure, and changes, alternatives, and modifications can be made in the embodiments without departing from spirit, principles and scope of the present disclosure.

What is claimed is:

1. A data interaction method, comprising:

obtaining a real card information list of smart cover end by a smart cover, wherein the real
 5 card information list of smart cover end is a real card information list of real card manager end
 obtained from a real card manager by the smart cover, and the real card information list of real
 card manager end comprises real card information of real cards connected to the real card
 manager;

prompting the real card information list of smart cover end by the smart cover;

10 receiving a real card selecting instruction by the smart cover, determining a selected real card
 by the smart cover;

receiving first data sent from a transaction terminal by a simulation card, and sending the first
 data to the smart cover by the simulation card;

prompting the first data by the smart cover, receiving a confirming instruction for confirming
 15 that the first data is correct by the smart cover, and sending the first data to the real card manager
 by the smart cover; and

receiving the first data sent from the smart cover by the real card manager, and sending the
 first data to the selected real card by the real card manager.

2. The method according to claim 1, further comprising:

20 establishing a secure connection between the smart cover and the simulation card, and
 obtaining a first secure transmission key of smart cover end and a secure transmission key of
 simulation card end for secure data transmission between the smart cover and the simulation card.

3. The method according to claim 1 or 2, further comprising:

establishing a secure connection between the smart cover and the real card manager, and
 25 obtaining a second secure transmission key of smart cover end and a secure transmission key of
 real card manager end for secure data transmission between the smart cover and the real card
 manager.

4. The method according to claim 2, before establishing a secure connection between the
 smart cover and the simulation card, further comprising:

30 performing a binding operation between the smart cover and the simulation card.

5. The method according to claim 3, before establishing a secure connection between the

smart cover and the real card manager, further comprising:

performing a binding operation between the smart cover and the real card manager.

6. The method according to claim 3,

before establishing a secure connection between the smart cover and the real card manager,

5 further comprising:

sending a login request to the real card manager by the smart cover; and

after establishing a secure connection between the smart cover and the real card manager,

further comprising:

performing a first processing on a received login password by the smart cover using the

10 second secure transmission key of smart cover end to obtain a first processed password, and

sending the first processed login password to the real card manager by the smart cover;

receiving data sent from the smart cover by the real card manager, performing a second

processing on received data by the real card manager using the secure transmission key of real

card manager end to obtain second processed data, and verifying a correctness of the second

15 processed data by the real card manager;

after the real card manager verifies that the second processed data passes verification, making the smart cover login to the real card manager.

7. The method according to claim 6, wherein performing a second processing on received data by the real card manager using the secure transmission key of real card manager end to obtain

20 second processed data and verifying a correctness of the second processed data by the real card

manager comprises:

performing the second processing on the received data by the real card manager using the secure transmission key of real card manager end to obtain a password to be verified;

determining, by the real card manger, whether the password to be verified is an alarm

25 password;

if the password to be verified is an alarm password, performing an alarm operation by the real card manager after verified the password to be verified successful;

if the password to be verified is a login password rather than an alarm password, determining that the password to be verified passes the verification by the real card manager.

30 8. The method according to claim 6, further comprising:

detecting, by the real card manager, the real cards connected to the real card manager;

after the real card manager detects the real cards connected to the real card manager, obtaining real card information of the real cards by the real card manager, wherein the real card information comprises at least a card number;

5 after the real card manager obtains the real card information of the real cards, generating the real card information list of real card manager end by the real card manager.

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

generating an identification list of real card manager end by the real card manager, wherein identifications in the identification list of real card manager end have a one-to-one correspondence with the real card information in the real card information list of real card manager end.

10 10. The method according to claim 1, wherein receiving a real card selecting instruction by the smart cover and determining a selected real card by the smart cover comprises:

receiving the real card selecting instruction by the smart cover, and obtaining a selected identification by the smart cover, wherein the selected identification is configured to indicate the selected real card;

15 sending the selected identification to the real card manager by the smart cover;

determining the selected real card corresponding to the selected identification by the real card manager from the real cards connected to the real card manager according to the selected identification.

11. The method according to claim 2, wherein,

20 after the secure connection is established between the smart cover and the simulation card, the simulation card performs a first processing on the first data using the secure transmission key of simulation card end and sends first data obtained after the first processing to the smart cover, and after receiving the first data obtained after the first processing, the smart cover performs a second processing using the first secure transmission key of smart cover end; the smart cover performs a
25 first processing on second data using the first secure transmission key of smart cover end and sends second data obtained after the first processing to the simulation card, and after receiving the second data obtained after the first processing, the simulation card performs a second processing using the secure transmission key of simulation card end.

12. The method according to claim 3,

30 after the secure connection is established between the smart cover and the real card manager, the smart cover performs a first processing on the first data using the second secure transmission

key of smart cover end and sends first data obtained after the first processing to the real card manager, and after receiving the first data obtained after the first processing, the real card manager performs a second processing using the secure transmission key of real card manager end; the real card manager performs a first processing on second data using the secure transmission key of real card manager end and sends the second data obtained after the first processing to the smart cover, and after receiving the second data obtained after the first processing, the smart cover performs a second processing using the second secure transmission key of smart cover end.

13. The method according to any one of claims 1 to 12, wherein the real card manager sets ON and/or OFF for read and write access to the real card information of the real cards connected to the real card manager according to security levels of the real cards.

14. The method according to any one of claims 1 to 13, wherein the smart cover is a mobile device.

15. The method according to any one of claims 1 to 13, wherein the smart cover is a combination of a mobile device and an electronic signature token, or the smart cover is an electronic signature token.

16. A data interaction system, comprising a simulation card, a smart cover and a real card manager, wherein

the smart cover is configured to obtain a real card information list of smart cover end, to prompt the real card information list of smart cover end, to receive a real card selecting instruction, and to determine a selected real card, in which the real card information list of smart cover end is a real card information list of real card manager end obtained by the smart cover from the real card manager, and the real card information list of real card manager end comprises real card information of real cards connected to the real card manager;

the simulation card is configured to receive first data sent by a transaction terminal, and to send the first data to the smart cover;

the smart cover is further configured to prompt the first data, to receive a confirming instruction for confirming that the first data is correct, and to send the first data to the real card manager; and

the real card manager is configured to receive the first data sent by the smart cover, and to send the first data to the selected real card.