

DATA INTERACTION METHOD AND SYSTEM

FIELD

The present disclosure relates to electronic information security technology field, 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 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 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.

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 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 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 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.

In addition, the data interaction method further comprising: 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, establishing a secure connection between the smart cover and the simulation card includes: sending a first secure connection instruction for indicating the establishment of a secure connection to the simulation card by the smart cover, wherein the first secure connection instruction includes: encrypting a first binding factor as well as a first connection random factor to get a first connection ciphertext using public key of the simulation card in the certificate of a simulation card by the smart cover, signing a first binding factor as well as a first connection random factor to get a first connection signature message using private key of the smart cover; the simulation card receives the first secure connection instruction, decrypts the first connection ciphertext using the private key of the simulation card to get the first binding factor and the first connection random factor; the simulation card verifies the first connection signature message using the public key of the smart cover in the certification of the smart cover, the first binding factor and the first connection random factor; the simulation card verification of one connection after the signature is correct, verify the ferrule end I bound to decrypt the same factor and a simulation card-binding factor; the simulation card to generates the second random factor after verifies that the first binding decryption factor is the same as the simulation card end binding factor; The simulation card encrypts the first connection random decryption factor and the second connection random factor using the smart cover public key in the smart cover certificate to obtain the second connection ciphertext; the simulation card sends the response of a secure connection to the set of cards, in which, the secure connection response include: the second connection signature ciphertext and the second connection; The smart covers the first secure connection response, decrypts the second connection ciphertext with the key of the smart cover, obtains the decrypted

first connection random decryption factor and the second connection random decryption factor;
card using a simulation card simulation card public key in the certificate, to decrypt the connection
of random factors and factors on the next connection for random decryption signature verification;
After confirming that the second connection signature is correct, verify that the first connection
5 random decryption factor is the same as the first connection random factor; the first connection
random decryption factor is decrypted and the first connection random factor is the same, and the
first secure transmission key between the card and the simulation card is generated by using the
second connection random decryption factor at least; the simulation card generates an simulation
card-side secure transmission key between the smart cover and the simulation card using at least
10 the second connection random factor.

In addition, establishing a secure connection between the smart cover and the simulation card
includes: the smart cover receives third random factors generated by simulation card and
simulation card unique identification card sent by simulation card; smart cover sends simulation
card used to indicate the second secure connection instructions to establish a secure connection,
15 wherein the second secure connection instruction comprises: a card uniquely identifying a third
connection cipher obtained by encrypting the third connection random factor and the generated
fourth connection random factor using the simulation card public key in the simulation card
certificate, the third connection signature obtained by signing the third connection random factor
and the fourth connection random factor using the smart cover private key; the simulation card
20 receives the second secure connection instruction to determine whether the smart cover uniquely
identifies whether it is in the simulation card end binding list; if the card is uniquely identified in
the simulation card end binding list, the simulation card decrypts the third connection cipher using
the simulation card private key, obtains the third connection random decryption factor and the
fourth connection random decryption factor; the simulation card uses the smart cover public key in
25 the smart cover certificate, the third connection random decryption factor and the fourth
connection random decryption factor to verify the third connection signature; after verifying that
the third connection signature is correct, verify that the third connection random decryption factor
is the same as the third connection random factor; if the third connection random decryption factor
is the same as the third connection random factor, the simulation card uses the simulation card
30 private key to sign the fourth connection random decryption factor and the fourth connection
random decryption factor to obtain the fourth connection signature; the simulation card sends a

second secure connection response to the smart cover, wherein the second secure connection response comprises: a fourth connection signature; the smart cover receives the second secure connection response, verifies the fourth connection signature using the simulation card public key, the third connection random factor and the fourth connection random factor in the simulation card certificate; the first secure transmission key is generated by using the fourth connection random factor and the first binding factor of the smart cover to generate the first secure transmission key between the smart cover and the simulation card; the simulation card generates the simulation card-side secure transmission key between the card and the simulation card using at least the fourth connection random decryption factor and the simulation card end binding factor; the smart cover sends the first connection random factor and the fourth connection random factor to the simulation card by using the first secure transmission key of the smart cover end; the simulation card sends the first connection random decryption factor and the fourth connection random decryption factor to the card case by using the simulation card side secure transmission key; the smart cover receives the data sent by the simulation card and performs the second processing on the received data using the first secure transmission key of the smart cover to compare the second processed data with the third connection random factor and the fourth connection random factor the same; and the second processing is compared with the third connection random decryption factor and the fourth connection random decryption factor whether the data of the second processing is compared with the third connection random decryption factor the same.

In addition, the data interaction method further comprising: establishing a secure 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, establishing a secure connection between the smart cover and the simulation card includes: the smart cover to send to the real card manager a third secure connection instruction for indicating the establishment of a secure connection, wherein the third secure connection instruction comprises: a smart cover encrypting the fifth connection using the real card manager public key in the real card manager certificate to encrypt the second binding factor and the generated fifth connection random factor the second connection signature obtained by signing the second binding factor and the fifth connection random factor using the smart cover private key; the real card manager receives the third secure connection instruction, decrypts the fifth connection

cipher using the real card manager private key, obtains the second binding decryption factor and the fifth connection random decryption factor; the real card manager validates the fifth connection signature using the smart cover public key, the second binding decryption factor and the fifth connection random decryption factor in the smart cover certificate; after the real card manager
5 verifies that the fifth connection is correct, verify that the second binding decryption factor is the same as the true card manager binding factor; the real card manager verifies that the second binding decryption factor is the same as the real card manager end binding factor, resulting in a sixth join random factor; the real card manager obtains the sixth connection ciphertext by encrypting the fifth connection random decryption factor and the sixth connection random factor
10 using the card public key in the smart cover certificate, and using the real card manager private key to the fifth connection random decryption factor And a sixth connection random factor to obtain a sixth connection signature; the real card manager sends a third secure connection response to the smart cover, wherein the third secure connection response comprises: a sixth connection ciphertext and a sixth connection signature; the smart covers the third secure connection response,
15 decrypts the sixth connection ciphertext with the card private key, obtains the decrypted fifth connection random decryption factor and the sixth connection random decryption factor; the smart cover validates the sixth connection signature using the real card manager public key in the real card manager certificate, the decrypted fifth connection random decryption factor, and the sixth connection random decryption factor; after confirming that the sixth connection signature is
20 correct, verify that the fifth connection random decryption factor and the fifth connection random factor are the same; the fifth connection random decryption factor is decrypted and the fifth connection random factor is the same, and at least the sixth connection random decryption factor is used to generate the second secure transmission key between the smart cover and the real card manager; the real card manager uses at least the sixth connection random factor to generate a real
25 card manager secure transport key between the smart cover and the real card manager.

In addition, the smart cover with the real card manager to establish a secure connection includes: the card receives the real card manager to send the real card manager generated by the seventh connection random factor and the real card manager uniquely identifies; a fourth secure connection instruction for indicating the establishment of a secure connection is sent to the real
30 card manager by the smart cover, wherein the fourth secure connection instruction comprises: a smart cover unique identifier, the smart cover utilizes the real card manager public key in the real

card manager certificate to the seventh connection random factor and The seventh connection ciphertext obtained by encrypting the generated eighth connection random factor, the second connection signature obtained by signing the seventh connection random factor and the eighth connection random factor with the smart cover private key; the real card manager receives the
5 fourth secure connection command to determine whether the smart cover uniquely identifies is in the real card manager side binding list; if the smart cover uniquely identifies is in the real card manager end binding list, the real card manager utilizes the real card manager private key decrypts the seventh connection ciphertext, obtains the seventh connection random decryption factor and the eighth connection random decryption factor; the real card manager validates the seventh
10 connection signature using the smart cover public key in the smart cover certificate, the seventh connection random decryption factor, and the eighth connection random decryption factor; the real card manager verifies whether the random decryption factor is the same as the seventh connection random factor after verifies that the seventh connection signature is correct; if the seventh connection random decryption factor is the same as the seventh connection random factor, the real
15 card manager uses the real card manager private key to sign the seventh connection random decryption factor and the eighth connection random decryption factor to obtain the eighth connection signature; the real card manager sends a fourth secure connection response to the smart cover, wherein the fourth secure connection response includes: the eighth connection signature; the smart cover receives the fourth secure connection response, uses the real card manager public key
20 in the real card manager certificate, the seventh connection random factor and the eighth connection random factor to verify the eighth connection signature; after confirming that the eighth connection signature is correct, at least the second connection random factor and the second binding factor of the card are used to generate the second secure transmission key between the smart cover and the real card manager. the real card manager generates a real card manager secure
25 transport key between the smart cover and the real card manager at least using the eighth connection random decryption factor and the real card manager end binding factor; the smart cover sends the seventh connection random factor and the eighth connection random factor to the real card manager after first processing using the second security transmission key; the real card manager sends the seventh connection random decryption factor and the eighth connection random
30 decryption factor after first processing using the real card manager side secure transmission key; the card receives the data sent by the real card manager and performs the second processing on the

received data using the second secure transmission key of the smart cover, compares whether the second processed data is the same as the seventh connection random factor and the eighth connection random factor; the real card manager receives the data sent by the smart cover and uses the real card manager side secure transmission key to perform the second processing on the received data, compares the second processed data with the seventh connection random decryption factor and the eighth connection random decryption factor.

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

In addition, the binding operation of the card and the simulation card includes: the smart cover receives a trigger command for indicating the binding with the simulation card; the smart cover sends the first binding instruction to the simulation card, wherein the first binding command includes: the first binding random factor generated by the smart cover, the smart cover certificate and the unique identifier of the smart cover; the simulation card receives the first binding instruction, uses the root certificate to verify the smart cover certificate; after the simulation card validates the smart cover certificate, the second binding random factor is generated; the simulation card encrypts the first binding random factor and the second binding random factor to obtain the first binding ciphertext, signatures the first binding random factor and the second binding random factor to obtain the first binding signature; the simulation card sends the first binding response to the simulation card, wherein the first binding response includes a first binding cipher, a first binding signature, an simulation card certificate, and an simulation card unique identifier; the smart cover receives the first binding response, verifies the simulation card certificate with the root certificate; after the verification of the simulation card certificate, the first binding ciphertext is decrypted by the smart cover private key, to obtain the first binding random decryption factor and the second binding random decryption factor; the smart cover verifies the first binding signature using the simulation card public key in the simulation card certificate, the first binding random decryption factor and the second binding random decryption factor; the smart cover verifies that the first binding random decryption factor is the same as the first binding random factor after confirming that the first binding signature is correct; if the first binding random decryption factor is the same as the first binding random factor, indicating the simulation card unique identification by the smart cover; the smart cover receives the triggering command for confirming the simulation

card unique identification is correct, signs the first binding random factor and the second binding random decryption factor with the smart cover private key to obtain the second binding signature, and stores the simulation card unique identification, the simulation card certificate and the first binding factor of the smart cover to the first binding list of the smart cover, wherein the first binding factor of the smart cover is the second binding random decryption factor; the smart cover sends the second binding signature to the simulation card; the simulation card receives the second binding signature, utilizes the smart cover public key in the smart cover certificate, the first binding random factor, and the second binding random factor to verify the second binding signature; the simulation card verifies that the second binding signature is correct, stores the smart cover unique identification, the smart cover certificate, and the simulation card end binding factor to the simulation card end binding list, wherein the simulation card end binding factor is the second binding random factor.

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

In addition, the binding operation performed by the smart cover with the real card manager includes: the smart cover receives the trigger command for indicating the binding with the real card manager; the smart cover sends the second binding instruction to the real card manager over the wireless network, wherein the second binding instruction comprises: a third binding random factor generated by the smart cover, the smart cover certificate, and a smart cover unique identification; the real card manager receives the second binding instruction and verifies the smart cover certificate with the root certificate; the real card manager generates the fourth binding random factor after verifies that the certificate is legal; the real card manager encrypts the third binding random factor and the fourth bound random factor using the smart cover public key in the smart cover certificate to obtain the second binding ciphertext, sign the third binding random factor and the fourth binding random factor using the real card manager private key to obtain the third binding signature; the real card manager sends a second binding response to the smart cover via the wireless network, Wherein the second binding response includes a second binding ciphertext, a third binding signature, a real card manager certificate, and a real card manager unique identification; the smart cover receives the second binding response and verifies the real card manager certificate using the root certificate; after confirming that the real card manager

certificate is valid, the second binding ciphertext is decrypted by the card private key to obtain the third binding random decryption factor and the fourth binding random decryption factor; the smart cover verifies the third binding signature using the real card manager public key in the real card manager certificate, the third binding random decryption factor, and the fourth binding random decryption factor; after verifying that the third binding is correct, the smart cover verifies whether the third binding random decryption factor is the same as the third binding random factor; the smart cover prompts the real card manager unique identification after verifies that the third binding random decryption factor is the same as the third binding random factor; the smart cover receives a trigger command used to confirm that the real card manager unique identification, sign the third binding random factor and the fourth binding random decryption factor with the smart cover private key, obtains the fourth binding signature, and stores the real card manager unique identification, the real card manager certificate and the second binding factor of the smart cover to the second binding list of the smart cover, wherein the second binding factor of the card is the fourth binding random decryption factor; the smart cover sends the fourth binding signature to the real card manager; the real card manager receives the fourth binding signature, verifies the fourth binding signature using the smart cover public key in the smart cover certificate, the third binding random factor and the fourth binding random factor; after the real card manager verifies the fourth binding signature is correct, stores the smart cover unique identification, the smart cover certificate, and the real card manager binding factor to the real card manager side binding list, wherein the real card manager side binding factor is the fourth binding random factor.

In addition, before establishing a secure connection between the smart cover and the real card manager, the data interaction method 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 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 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 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 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.

In addition, the data interaction method 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; 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.

In addition, the data interaction method 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.

In addition, after the smart cover logs into the real card manager, the data interaction method further includes: the smart cover searches the smart cover identification list; if the smart cover finds the smart cover of identification list, sends the smart cover of identification list to the real card manager after first processing with the second security transmission key, the real card manager receives the data sent by the smart covers, performs a second processing to the received data using the real card manager side secure transmission key, judges whether the second processed data is the same as the real card manager side identification list stored by the real card manager, if not, the real card manager performs the first processing to the update command and the update data using the real card manager secure transmission key and sends the processed data to the smart cover, the smart cover receives the data sent by the real card manager, performs the second processing to the received data using the second security transmission key, updates the real

card information list in the smart cover end; if the smart cover does not find the smart cover identification list, the default identification is sent to the real card manager after performs the first processing using the second secure transmission key of the smart cover, the real card manager receives the data sent by the smart covers, performs the second processing to the received data using the real card manager side secure transmission key, if the real card manager determines that the second processed data is used to indicate that the smart cover side does not store the smart cover end identification list, sends the update instruction and the update data after first processing with the real card manager side secure transmission to the smart cover, the card receives the data sent by the real card manager, uses the second security transmission key of the card to performs the second processing on the received data, updates the smart cover real card information list.

In addition, after the smart cover login real card manager, the data interaction method further includes: the real card manager using real card manager-side security transmission key to perform the first processing on the real card manager side identification list and sent to the smart cover; the smart cover receives the data sent by the real card manager, uses the second secure transmission key of the smart cover to perform the second processing on the received data, determines whether the second processed data is the same as the smart cover identification list stored by the smart cover; if not, the smart cover sends the update request to the real card manager; the real card manager receives the update request, uses the real card manager side security transmission key to perform the first processing to the update instruction and the update data, sends to the smart cover; the card receives the data sent by the real card manager, uses the second security transmission key of the card to carry on the second processing to the received data, updates the smart cover real card information list.

In addition, the smart cover also includes a heart sleep sleep mode, wherein the heartbeat sleep mode is a low power non-operating mode, the data interaction method further comprises: the smart cover sends the detection information to the real card manager every first preset time in the heartbeat sleep mode; the real card manager receives the detection information, sends the response information to the smart cover; if the smart cover does not receive the response message within the second preset time, disconnects the secure connection between the smart cover and the real card manager; if the card receives a response message within the second preset time, the secure connection of the smart cover to the actual card manager is maintained.

In addition, if the smart cover receives the response information within the second preset time

and the response information further contains the update prompt information, the data interaction method further comprises: the smart cover stores update prompt information; After the smart cover enters the work mode from the heart sleep mode, the smart cover sends the update trigger request to the real card manager; the real card manager receives the update trigger request, uses the real card manager side secure transmission key to carry on the first processing to the real card manager side identification list and sends to the smart cover; the card receives the data sent by the real card manager, performs the second processing on the received data using the second secure transmission key, determines whether the second processed data is the same as the smart cover identification list stored in the smart cover; if not, the smart cover sends an update request to the real card manager; the real card manager receives the update request, sends the data to the smart cover after first processing on the update instruction and the update data using the real card manager side secure transmission key; the smart cover receives the data sent by the real card manager, and then uses the second secure transmission key of the card to perform the second processing on the received data, and then updates the real card information list.

In addition, if the card receives the response information within the second preset time and the response information further contains the update prompt information, the data interaction method further comprises: the smart cover stores update prompt information; After the smart cover enters the work mode from the heart sleep mode, the smart cover uses the second security transmission key of the card to carry out the first processing to the smart cover end identification list and sends it to the real card manager; the real card manager receives the data sent by the smart cover, uses the real card manager side secure transmission key to carry out second processing on the received data, determines whether the second processed data is the same as the real card manager side identity list stored on the real card manager; if not, the real card manager uses the real card manager secure transmission key to perform the first processing on the update command and the update data, and then send it to the smart cover; the smart cover receives the data sent by the real card manager, and then uses the second secure transmission key of the card to perform the second processing on the received data, updates the real card information list of the smart cover.

In addition, 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, in which the selected identification is configured to indicate the selected 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.

In addition, the data interaction method further includes: the smart cover sends at least the smart cover certificate to a update platform; the update platform generates the first update encryption key; the update platform encrypts the smart cover installation package with the first update encryption key to obtain the first installation package ciphertext; the update platform uses the update platform private key to sign the first installation package to obtain the first installation package signature; the update platform encrypts the first update encryption key using the smart cover public key in the smart cover certificate to obtain the first update encryption key ciphertext; the update platform sends the smart cover update information to the smart cover, wherein the card update information includes: update the platform certificate, the first installation package ciphertext, the first installation package signature, and the first update encryption key ciphertext; smart cover receives smart cover update information, use the root certificate to verify the update platform certificate; after confirming the update platform certificate, the first installation package signature is checked by using the update platform public key in the update platform certificate; After confirming that the first installation package signature is correct by the smart cover, the first encryption key is decrypted by the card private key to obtain the first decryption key; the smart cover decrypts the first installation package using the first decryption key to obtain the package application package; the smart cover verifies whether the data format of the package installation package is correct; if so, the smart cover installs according to the application package.

In addition, the data interaction method further includes: the smart cover obtains the simulation card certificate from the simulation card, sends at least the simulation card certificate to the update platform; the update platform generates the second update encryption key; the update platform encrypts the simulation card application installation package with the second update encryption key to obtain the second installation package ciphertext; the update platform uses the update platform private key to sign the second installation package to obtain the second installation package signature; the update platform encrypts the second update encryption key using the simulation card public key in the simulation card certificate to obtain the second update encryption key ciphertext; the update platform sends the simulation card update information to the smart cover, wherein the simulation card update information includes: updating the platform

certificate, the second installation package ciphertext, the second installation package signature, and the second update encryption key ciphertext; the smart cover receives the simulation card update information and sends it to the simulation card; the simulation card receives the simulation card update information sent by the smart cover, uses the root certificate to verify the update platform certificate; after the simulation card verifies the update platform certificate, uses the update platform public key in the update platform certificate to verify the second installation package signature; after the simulation card verifies that the second installation package signature is correct, decrypts the second update encryption key ciphertext using the simulation card private key to obtain the second decryption key; the simulation card decrypts the second installation package cipher using the second decryption key to obtain the simulation card application installation package; simulation card verification whether the data format of the card application installation package is correct; if the simulation card verifies that the data for the format of the simulation card application installation package correctly, the simulation card is installed according to the simulation card application installation package.

15 In addition, the data interaction method further includes: the real card manager sends at least the real card manager certificate to the update platform; the update platform generates the third update encryption key; the update platform utilizes the third update encryption key to the real card manager application installation package for encryption to obtain the third installation package; the update platform uses the update platform private key to sign the third installation package to obtain the third installation package signature; update the platform using the real card manager certificate in the real card manager to obtain the third update encryption key; the update platform sends the real card manager update information to the real card manager, wherein the real card manager update information includes: updating the platform certificate, the third installation package ciphertext, third install package signature and third update encryption key cipher text; real card manager receives real card manager update information, uses root certificate to verify update platform certificate; real card manager verifies update platform certificate passes , The use of updated platform certificate in the update platform public key to the first The real card manager verifies that the third installation package is signed correctly, decrypts the third update encryption key using the real card manager private key, obtains the third decryption key; the real card manager uses the Three decryption key decryption third install package cipher, get real card manager application installation package; real card manager verifies that the real card manager

application installs the data format of the package is correct; if the real card manager verifies the real card management the application package for the application package is properly formatted and the real card manager is installed according to the real card manager application installation package.

5 In addition, 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
10 cover performs a 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.

 In addition, after the secure connection is established between the smart cover and the real
15 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
20 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.

 In addition, the first processing includes: an encryption process, the second process comprising: a decryption process; or the first processing includes: a verification calculation
25 process, the second process comprising: a verification verification calculation process; or the first processing comprises: encryption and verification calculation processing, the second process comprising: decryption and verification verification calculation processing.

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

 In addition, the smart covers the simulation card out of the effective communication range of

the card, the safety tips.

In addition, the smart cover is a mobile device.

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

5 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 provided. The system includes a simulation card, a smart cover and a real card manager. The smart cover is
10 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 includes real card information of real
15 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. The real card manager is configured to receive the first data sent by the smart cover, and to send the first data to the
20 selected real card.

In addition, the smart cover, is further configured to the establishment of a secure connection with the simulation card to obtain the first secure transmission key of smart cover end for secure data transmission between the smart cover and the simulation card; the simulation card, is further configured to establish a secure connection with the smart cover to obtain the secure transmission
25 key of simulation card for secure data transmission between the smart cover and the simulation card.

In addition, the card holder is specifically configured to send to the simulation card a first secure connection instruction for indicating the establishment of a secure connection, wherein the first secure connection instruction includes: encrypting a first binding factor as well as a first
30 connection random factor to get a first connection ciphertext using public key of the simulation card in the certificate of a simulation card by the smart cover, signing a first binding factor as well

as a first connection random factor to get a first connection signature message using private key of the smart cover; the simulation card is specifically configured to receive the first secure connection instruction, decrypt the first connection ciphertext using the private key of the simulation card to get the first binding factor and the first connection random factor; the simulation card is specifically configured to verify the first connection signature message using the public key of the smart cover in the certification of the smart cover, the first binding factor and the first connection random factor; the simulation card verification of one connection after the signature is correct, the simulation card is configured to verify the ferrule end I bound to decrypt the same factor and a simulation card-binding factor; the simulation card to verify the ferrule end I bound to decrypt and a simulation card after the same end-binding factors, generating the next random factor; the simulation card using the smart covers the public key in the certificate set of cards to connect the random decryption factor and the random factor to get the next connection to encrypt the ciphertext, the simulation card is configured to decrypt the private key on the one connected to a random factor and the random factor to get the next connection to sign the signature; the simulation card is configured to send the response of a secure connection to the set of cards, in which, the secure connection response include: the next connection signature ciphertext and the next connection; smart cover in response to receiving a secure connection, the simulation card is configured to use the private key of smart covers to decrypt the ciphertext for the next connection, access to decrypt the connection of random factors and the random decryption factor;

the card holder is specifically configured to use a simulation card simulation card public key in the certificate, to decrypt the connection of random factors and factors on the next connection for random decryption signature verification; to verify the connection after the signature is correct, the connection to validate decrypted random decryption factor and the random factor in whether or not the same; the smart cover is specifically configured to verify connection of random and decryption of the same, the factor and the random factor using at least two connections for random decryption factors generate a set of cards and smart cover of cards between the end of one key transmission; the simulation card is specifically configured to use at least two connection between random generate a set of cards and a simulation card simulate card-key transmission.

In addition, the smart cover is specifically configured to receive third random factors generated by simulation card and simulation card unique identification card sent by simulation card; send to simulation card used to indicate the second secure connection instructions to

establish a secure connection, wherein the second secure connection instruction comprises: a card uniquely identifying a third connection cipher obtained by encrypting the third connection random factor and the generated fourth connection random factor using the simulation card public key in the simulation card certificate, the third connection signature obtained by signing the third connection random factor and the fourth connection random factor using the smart cover private key; the simulation card is specifically configured to receive the second secure connection instruction to determine whether the card holder uniquely identifies whether it is in the simulation card end binding list; if the card is uniquely identified in the simulation card end binding list, the simulation card is configured to decrypt the third connection cipher using the simulation card private key, obtain the third connection random decryption factor and the fourth connection random decryption factor; the simulation card is configured to use the smart cover public key in the smart cover certificate, the third connection random decryption factor and the fourth connection random decryption factor to verify the third connection signature; after verifying that the third connection signature is correct, the simulation card is configured to verify that the third connection random decryption factor is the same as the third connection random factor; if the third connection random decryption factor is the same as the third connection random factor, the simulation is configured to use the simulation card private key to sign the fourth connection random decryption factor and the fourth connection random decryption factor to obtain the fourth connection signature; the simulation card is configured to send a second secure connection response to the card holder, wherein the second secure connection response comprises: a fourth connection signature; the smart cover is specifically configured to receive the second secure connection response, verify the fourth connection signature using the simulation card public key, the third connection random factor and the fourth connection random factor in the simulation card certificate; the first secure transmission key is generated by using the fourth connection random factor and the first binding factor of the card holder to generate the first secure transmission key between the smart cover and the simulation card; the simulation card is specifically configured to generate the simulation card-side secure transmission key between the card and the simulation card using at least the fourth connection random decryption factor and the simulation card end binding factor; the card holder sends the first connection random factor and the fourth connection random factor to the simulation card by using the first secure transmission key of the smart cover end; the simulation card is specifically configured to send the first connection random decryption factor

and the fourth connection random decryption factor to the card case by using the simulation card side secure transmission key; the smart cover is specifically configured to receive the data sent by the simulation card and performs the second processing on the received data using the first secure transmission key of the card holder to compare the second processed data with the third connection random factor and the fourth connection random factor the same; and the second processing is compared with the third connection random decryption factor and the fourth connection random decryption factor whether the data of the second processing is compared with the third connection random decryption factor the same.

In addition, the smart cover, is further configured to the establishment of a secure connection with the simulation card to obtain the second secure transmission key of smart cover end for secure data transmission between the smart cover and the simulation card; the simulation card, is further configured to establish a secure connection with the smart cover to obtain the secure transmission key of simulation card for secure data transmission between the smart cover and the simulation card.

In addition, the smart cover is specifically configured to send to the real card manager a third secure connection instruction for indicating the establishment of a secure connection, wherein the third secure connection instruction comprises: a card holder encrypting the fifth connection using the real card manager public key in the real card manager certificate to encrypt the second binding factor and the generated fifth connection random factor the second connection signature obtained by signing the second binding factor and the fifth connection random factor using the card holder private key; the real card manager is specifically configured to receive the third secure connection instruction, decrypt the fifth connection cipher using the real card manager private key, obtain the second binding decryption factor and the fifth connection random decryption factor; the real card manager is specifically configured to validate the fifth connection signature using the smart cover public key, the second binding decryption factor and the fifth connection random decryption factor in the smart cover certificate; after the real card manager verifies that the fifth connection is correct, verify that the second binding decryption factor is the same as the true card manager binding factor; the real card manager is specifically configured to verify that the second binding decryption factor is the same as the real card manager end binding factor, generate a sixth join random factor; the real card manager is specifically configured to obtain the sixth connection ciphertext by encrypting the fifth connection random decryption factor and the sixth connection

random factor using the card public key in the smart cover certificate, and using the real card manager private key to the fifth connection random decryption factor and a sixth connection random factor to obtain a sixth connection signature; the real card manager is specifically configured to send a third secure connection response to the card holder, wherein the third secure connection response comprises: a sixth connection ciphertext and a sixth connection signature; the smart cover is specifically configured to receive the third secure connection response, decrypts the sixth connection ciphertext with the card private key, obtain the decrypted fifth connection random decryption factor and the sixth connection random decryption factor; the card holder is specifically configured to validate the sixth connection signature using the real card manager public key in the real card manager certificate, the decrypted fifth connection random decryption factor, and the sixth connection random decryption factor; after confirming that the sixth connection signature is correct, the card holder is specifically configured to verify that the fifth connection random decryption factor and the fifth connection random factor are the same; the fifth connection random decryption factor is decrypted and the fifth connection random factor is the same, and at least the sixth connection random decryption factor is used to generate the second secure transmission key between the smart cover and the real card manager; the real card manager is specifically configured to use at least the sixth connection random factor to generate a real card manager secure transport key between the card holder and the real card manager.

In addition, the smart cover is specifically configured to receive the real card manager to send the real card manager generated by the seventh connection random factor and the real card manager uniquely identifies; a fourth secure connection instruction for indicating the establishment of a secure connection is sent to the real card manager by the smart cover, wherein the fourth secure connection instruction comprises: a card holder unique identifier, the card holder utilizes the real card manager public key in the real card manager certificate to the seventh connection random factor and The seventh connection ciphertext obtained by encrypting the generated eighth connection random factor, the second connection signature obtained by signing the seventh connection random factor and the eighth connection random factor with the card holder private key; the real card manager is specifically configured to receive the fourth secure connection command to determine whether the card holder uniquely identifies is in the real card manager side binding list; if the card holder uniquely identifies is in the real card manager end binding list, the real card manager is specifically configured to utilize the real card manager

private key decrypts the seventh connection ciphertext, obtains the seventh connection random decryption factor and the eighth connection random decryption factor; the real card manager is specifically configured to validate the seventh connection signature using the smart cover public key in the smart cover certificate, the seventh connection random decryption factor, and the eighth connection random decryption factor; the real card manager is specifically configured to verify whether the random decryption factor is the same as the seventh connection random factor after verifies that the seventh connection signature is correct; if the seventh connection random decryption factor is the same as the seventh connection random factor, the real card manager is specifically configured to use the real card manager private key to sign the seventh connection random decryption factor and the eighth connection random decryption factor to obtain the eighth connection signature; the real card manager is specifically configured to send a fourth secure connection response to the card holder, wherein the fourth secure connection response includes: the eighth connection signature; the card holder is specifically configured to receive the fourth secure connection response, use the real card manager public key in the real card manager certificate, the seventh connection random factor and the eighth connection random factor to verify the eighth connection signature; after confirming that the eighth connection signature is correct, at least the second connection random factor and the second binding factor of the card are used to generate the second secure transmission key between the card holder and the real card manager; the real card manager is specifically configured to generate a real card manager secure transport key between the smart cover and the real card manager at least using the eighth connection random decryption factor and the real card manager end binding factor; the card holder is specifically configured to send the seventh connection random factor and the eighth connection random factor to the real card manager after first processing using the second security transmission key; the real card manager is specifically configured to send the seventh connection random decryption factor and the eighth connection random decryption factor after first processing using the real card manager side secure transmission key; the smart cover is specifically configured to receive the data sent by the real card manager and perform the second processing on the received data using the second secure transmission key of the card holder, compares whether the second processed data is the same as the seventh connection random factor and the eighth connection random factor; the real card manager is specifically configured to receive the data sent by the card holder and uses the real card manager side secure transmission key to perform the second processing on the

received data, compare the second processed data with the seventh connection random decryption factor and the eighth connection random decryption factor.

In addition, before establishing a secure connection between the card and the simulation card, the card is specifically configured to perform the binding operation with the simulation card.

5 In addition, the smart cover is specifically configured to receive a trigger command for indicating the binding with the simulation card; the smart cover is specifically configured to send the first binding instruction to the simulation card, wherein the first binding command includes: the first binding random factor generated by the card holder, the smart cover certificate and the unique identifier of the smart cover; the simulation card is specifically configured to receive the
10 first binding instruction, use the root certificate to verify the smart cover certificate; after the simulation card validates the smart cover certificate, the second binding random factor is generated; the simulation card is specifically configured to encrypt the first binding random factor and the second binding random factor to obtain the first binding ciphertext, signature the first binding random factor and the second binding random factor to obtain the first binding signature;
15 the simulation card is specifically configured to send the first binding response to the simulation card, wherein the first binding response includes a first binding cipher, a first binding signature, an simulation card certificate, and an simulation card unique identifier; the smart cover is specifically configured to receive the first binding response, verify the simulation card certificate with the root certificate; after the verification of the simulation card certificate, the first binding ciphertext is
20 decrypted by the card holder private key, to obtain the first binding random decryption factor and the second binding random decryption factor; the smart cover is specifically configured to verify the first binding signature using the simulation card public key in the simulation card certificate, the first binding random decryption factor and the second binding random decryption factor; the smart cover is specifically configured to verify that the first binding random decryption factor is
25 the same as the first binding random factor after confirming that the first binding signature is correct; if the first binding random decryption factor is the same as the first binding random factor, indicate the simulation card unique identification by the smart cover; the card holder is specifically configured to receive the triggering command for confirming the simulation card unique identification is correct, sign the first binding random factor and the second binding random
30 decryption factor with the smart cover private key to obtain the second binding signature, and store the simulation card unique identification, the simulation card certificate and the first binding factor

of the smart cover to the first binding list of the smart cover, wherein the first binding factor of the smart cover is the second binding random decryption factor; the smart cover is specifically configured to send the second binding signature to the simulation card; the simulation card is specifically configured to receive the second binding signature, utilize the smart cover public key in the smart cover certificate, the first binding random factor, and the second binding random factor to verify the second binding signature; the simulation card is specifically configured to verify that the second binding signature is correct, store the card holder unique identification, the smart cover certificate, and the simulation card end binding factor to the simulation card end binding list, wherein the simulation card end binding factor is the second binding random factor.

In addition, the smart cover is specifically configured to perform a binding operation with the real card manager before the card holder establishes a secure connection with the real card manager.

In addition, the smart cover is specifically configured to receive the trigger command for indicating the binding with the real card manager; the smart cover is specifically configured to send the second binding instruction to the real card manager over the wireless network, wherein the second binding instruction includes: a third binding random factor generated by the card holder, the smart cover certificate, and a card holder unique identification; the real card manager is specifically configured to receive the second binding instruction and verify the smart cover certificate with the root certificate; the real card manager is specifically configured to generate the fourth binding random factor after verifies that the certificate is legal; the real card manager is specifically configured to encrypt the third binding random factor and the fourth bound random factor using the smart cover public key in the smart cover certificate to obtain the second binding ciphertext, sign the third binding random factor and the fourth binding random factor using the real card manager private key to obtain the third binding signature; the real card manager is specifically configured to send a second binding response to the smart cover via the wireless network, wherein the second binding response includes a second binding ciphertext, a third binding signature, a real card manager certificate, and a real card manager unique identification; the smart cover is specifically configured to receive the second binding response and verify the real card manager certificate using the root certificate; after confirming that the real card manager certificate is valid, the second binding ciphertext is decrypted by the card private key to obtain the third binding random decryption factor and the fourth binding random decryption factor; the card holder is

specifically configured to verify the third binding signature using the real card manager public key in the real card manager certificate, the third binding random decryption factor, and the fourth binding random decryption factor; after verifying that the third binding is correct, the smart cover is specifically configured to verify whether the third binding random decryption factor is the same as the third binding random factor; the smart cover is specifically configured to prompt the real card manager unique identification after verifies that the third binding random decryption factor is the same as the third binding random facto; the smart cover is specifically configured to receive a trigger command used to confirm that the real card manager unique identification, sign the third binding random factor and the fourth binding random decryption factor with the smart cover private key, obtain the fourth binding signature, and stores the real card manager unique identification, the real card manager certificate and the second binding factor of the card holder to the second binding list of the card holder, wherein the second binding factor of the card is the fourth binding random decryption factor; the smart cover is specifically configured to send the fourth binding signature to the real card manager; the real card manager is specifically configured to receive the fourth binding signature, verify the fourth binding signature using the smart cover public key in the smart cover certificate, the third binding random factor and the fourth binding random factor; after the real card manager verifies the four binding signature is correct, store the smart cover unique identification, the smart cover certificate, and the real card manager binding factor to the real card manager side binding list, wherein the real card manager side binding factor is the fourth binding random factor.

In addition, the smart cover is specifically configured to send a login request to the real card manager before establishing a secure connection between the card and the real card manager; after establishing a secure connection between the card and the real card manager, the smart cover is specifically configured to send a login password after first processing with the second secure transmission key of the card holder; the real card manager is specifically configured to receive the data sent by the smart covers, conduct the second processing of the received data using the real card manager secure transmission key, verify the correctness of the data after the second processing; the card holder is specifically configured to log in to the real card manager after the real card manager verifies the second processed data.

In addition, the real card manager is specifically configured to obtain the password to be verified after the second processing of the received data using the real card manager secure

transmission key; the real card manager is specifically configured to judge whether the password to be verified is the alarm password; if the password to be verified is the alarm password, the real card manager is specifically configured to determine that the password passes verification and performs the alarm operation; if the password to be verified is not the alarm password and the login password, the real card manager is specifically configured to determine the password passes verification.

In addition, the real card manager is specifically configured to detect the real card connected to the real card manager; the real card manager is specifically configured to obtain the real card information of the real card after detecting the real card connected with the real card manager, wherein the real card information includes at least the card number; the real card manager is specifically configured to generate a real card information list of real card manager end after obtaining the real card information of the real card.

In addition, the real card manager is specifically configured to generate a real card manager side identification list, wherein the identification of the real card manager identification list and the real card information of the real card list in the real card manager are one by one correspondence.

In addition, after the smart cover logs into the real card manager, the smart cover is specifically configured to search the card holder identification list; if the smart cover finds the smart cover of identification list, send the smart cover of identification list to the real card manager after first processing with the second security transmission key; the real card manager is specifically configured to receive the data sent by the smart covers, perform a second processing to the received data using the real card manager side secure transmission key, judge whether the second processed data is the same as the real card manager side identification list stored by the real card manager, if not, the real card manager is specifically configured to perform the first processing to the update command and the update data using the real card manager secure transmission key and send the processed data to the smart cover, the smart cover is specifically configured to receive the data sent by the real card manager, perform the second processing to the received data using the second security transmission key, update the real card information list in the card holder end; if the card holder does not find the card holder identification list, the default identification is sent to the real card manager after performs the first processing using the second secure transmission key of the card holder, the real card manager is specifically configured to receive the data sent by the smart covers, perform the second processing to the received data using

the real card manager side secure transmission key, if the real card manager determines that the second processed data is used to indicate that the card holder side does not store the card holder end identification list, send the update instruction and the update data after first processing with the real card manager side secure transmission to the smart cover, the card is specifically
5 configured to receives the data sent by the real card manager, use the second security transmission key of the card to perform the second processing on the received data, update the card holder real card information list.

In addition, after the smart cover login real card manager, the real card manager is specifically configured to use real card manager-side security transmission key to perform the first
10 processing on the real card manager side identification list and sent to the smart cover; the smart cover is specifically configured to receive the data sent by the real card manager, use the second secure transmission key of the card holder to perform the second processing on the received data, determine whether the second processed data is the same as the smart cover identification list stored by the smart cover; if not, the smart cover is specifically configured to send the update
15 request to the real card manager; the real card manager is specifically configured to receive the update request, use the real card manager side security transmission key to perform the first processing to the update instruction and the update data, send to the smart cover; the smart cover is specifically configured to receive the data sent by the real card manager, use the second security transmission key of the card to carry on the second processing to the received data, update the card
20 holder real card information list.

In addition, the card holder also includes a heart sleep sleep mode, wherein the heartbeat sleep mode is a low power non-operating mode: the smart cover is specifically configured to send the detection information to the real card manager every first preset time in the heartbeat sleep mode; the real card manager is specifically configured to receive the detection information, send
25 the response information to the card holder; if the smart cover does not receive the response message within the second preset time, the smart cover is specifically configured to disconnect the secure connection between the card holder and the real card manager; if the card receives a response message within the second preset time, the secure connection of the card holder to the actual card manager is maintained.

30 In addition, if the smart cover receives the response information within the second preset time and the response information further contains the update prompt information, the smart cover is

specifically configured to store update prompt information; after the smart cover enters the work mode from the heart sleep mode, the smart cover is specifically configured to send the update trigger request to the real card manager; the real card manager is specifically configured to receive the update trigger request, use the real card manager side secure transmission key to carry on the first processing to the real card manager side identification list and send to the smart cover; the smart cover is specifically configured to receive the data sent by the real card manager, perform the second processing on the received data using the second secure transmission key, determine whether the second processed data is the same as the card holder identification list stored in the card holder; if not, the smart cover is specifically configured to send an update request to the real card manager; the real card manager is specifically configured to receive the update request, send the data to the smart cover after first processing on the update instruction and the update data using the real card manager side secure transmission key; the smart cover is specifically configured to receive the data sent by the real card manager, and then use the second secure transmission key of the card to perform the second processing on the received data, and then update the real card information list.

In addition, if the smart cover receives the response information within the second preset time and the response information further contains the update prompt information, the smart cover is specifically configured to store update prompt information; after the smart cover enters the work mode from the heart sleep mode, the card holder is specifically configured to use the second security transmission key of the card to carry out the first processing to the smart cover end identification list and sends it to the real card manager; the real card manager is specifically configured to receive the data sent by the card holder, use the real card manager side secure transmission key to carry out second processing on the received data, determine whether the second processed data is the same as the real card manager side identity list stored on the real card manager; if not, the real card manager use the real card manager secure transmission key to perform the first processing on the update command and the update data, and then send it to the smart cover; the smart cover is specifically configured to receive the data sent by the real card manager, and then use the second secure transmission key of the card to perform the second processing on the received data, update the real card information list of the card holder.

In addition, the smart cover is specifically configured to receive the real card selection command to determine the selected real card, wherein the selected identification is used to indicate

the selected real card; the smart cover is specifically configured to send the selected identification to the real card manager; the real card manager is specifically configured to determine the selected real card corresponding to the selected identification from the real card connected to the real card manager based on the selected identification.

5 In addition, the data interaction system also includes: a update platform; the smart cover is specifically configured to send at least the smart cover certificate to the update platform; the update platform is specifically configured to generate the first update encryption key; the update platform is specifically configured to encrypt the smart cover installation package with the first update encryption key to obtain the first installation package ciphertext; use the update platform
10 private key to sign the first installation package to obtain the first installation package signature; encrypt the first update encryption key using the smart cover public key in the smart cover certificate to obtain the first update encryption key ciphertext; send the smart cover update information to the card holder, wherein the card update information includes: update the platform certificate, the first installation package ciphertext, the first installation package signature, and the
15 first update encryption key ciphertext; smart cover is specifically configured to receive smart cover update information, use the root certificate to verify the update platform certificate; after confirming the update platform certificate, the first installation package signature is checked by using the update platform public key in the update platform certificate; after confirming that the first installation package signature is correct by the smart cover, the first encryption key is
20 decrypted by the card private key to obtain the first decryption key; the card holder is specifically configured to decrypt the first installation package using the first decryption key to obtain the package application package; the smart cover is specifically configured to verify whether the data format of the package installation package is correct; if so, the smart cover is specifically configured to install according to the application package.

25 In addition, the data interaction system also includes: a update platform; the smart cover is specifically configured to obtain the simulation card certificate from the simulation card, send at least the simulation card certificate to the update platform; the update platform is specifically configured to generate the second update encryption key; the update platform is specifically configured to encrypt the simulation card application installation package with the second update
30 encryption key to obtain the second installation package ciphertext; the update platform is specifically configured to use the update platform private key to sign the second installation

package to obtain the second installation package signature; the update platform is specifically configured to encrypt the second update encryption key using the simulation card public key in the simulation card certificate to obtain the second update encryption key ciphertext; the update platform is specifically configured to send the simulation card update information to the smart cover, wherein the simulation card update information includes: updating the platform certificate, the second installation package ciphertext, the second installation package signature, and the second update encryption key ciphertext; the smart cover is specifically configured to receive the simulation card update information and sends it to the simulation card; the simulation card is specifically configured to receive the simulation card update information sent by the smart cover, use the root certificate to verify the update platform certificate; after the simulation card verifies the update platform certificate, use the update platform public key in the update platform certificate to verify the second installation package signature; after the simulation card verifies that the second installation package signature is correct, decrypts the second update encryption key ciphertext using the simulation card private key to obtain the second decryption key; the simulation card is specifically configured to decrypt the second installation package cipher using the second decryption key to obtain the simulation card application installation package; simulation card verification whether the data format of the card application installation package is correct; if the simulation card verifies that the data for the format of the simulation card application installation package correctly, the simulation card is installed according to the simulation card application installation package.

In addition, the data interaction system also includes: a update platform; the real card manager is specifically configured to send at least the real card manager certificate to the update platform; the update platform is specifically configured to generate the third update encryption key; the update platform is specifically configured to utilize the third update encryption key to the real card manager application installation package for encryption to obtain the third installation package; the update platform is specifically configured to use the update platform private key to sign the third installation package to obtain the third installation package signature; update the platform using the real card manager certificate in the real card manager to obtain the third update encryption key; the update platform is specifically configured to send the real card manager update information to the real card manager, wherein the real card manager update information includes: updating the platform certificate, the third installation package ciphertext, third install package

signature and third update encryption key cipher text; real card manager is specifically configured to receive real card manager update information, use root certificate to verify update platform certificate; real card manager is specifically configured to verify update platform certificate passes , the use of updated platform certificate in the update platform public key to the first the real card manager verifies that the third installation package is signed correctly, decrypts the third update encryption key using the real card manager private key, obtains the third decryption key; the real card manager is specifically configured to use the third decryption key decryption third install package cipher, get real card manager application installation package; real card manager is specifically configured to verify that the real card manager application installs the data format of the package is correct; if the real card manager verifies the real card management the application package for the application package is properly formatted and the real card manager is installed according to the real card manager application installation package.

In addition, after the card holder establishes a secure connection with the simulation card, the simulation card is configured to sent the first data to the smart cover after the first processing using the simulation card-side secure transmission key, the smart cover is configured to receive the first data after the first processing, and the second processing is carried out using the smart cover-side secure transmission key; the second data sent by the smart cover to the simulation card is sent after the first processing using the card-side secure transmission key, the simulation card is configured to receive the second processed second data, and perform the second processing using the simulation card-side secure transmission key.

In addition, after the smart cover and the real card manager establishing a secure connection, the smart cover is configured to send the first data to the real card manager after first processing using the card-side security transmission key, the real card manager is configured to receive the first processed first data and performs the second processing using the real card manager side secure transmission key; the second data sent by the real card manager to the card holder is sent after the first card processing side using the real card manager side security transmission key by the real card manager, the smart cover is configured to receive the second processed data after the first processing, and perform the second processing using the card-side secure transmission key.

In addition, the first processing includes: an encryption process, the second process comprising: a decryption process; or the first processing includes: a verification calculation process, the second process comprising: a verification verification calculation process; or the first

processing comprises: encryption and verification calculation processing, the second process comprising: decryption and verification verification calculation processing.

In addition, the real card manager is configured to set the read and write permission of the real card information of the real card connected to the real card manager according to the security level of the real card.

In addition, the smart cover is configured to show the safety tips if the simulation card out of the effective communication range of the card.

In addition, the smart covers are mobile devices.

In addition, the card holder is a mobile device and an electronic signature token, or a card holder for an electronic signature token.

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 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

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 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;

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;

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;

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;

5 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;

10 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;

15 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;

20 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

25 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.

30 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 communications of two elements, which can be
10 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 transaction solution that is not only convenient for users' carrying, but also has high security. The data
15 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 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
20 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 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)
25 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 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
30 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. 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 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 in the real card manager that obtaining
5 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 network), or the like.

10 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 includes a decryption processing. Specifically, encryption alone ensures security of data transmission. When
15 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, verification alone ensures integrity of data transmission, preventing tampering. When integrity level of the data to be
20 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
25 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.

30 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.

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.

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.

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.

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 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 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 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 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 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 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 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.

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.

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.

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 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.

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 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 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 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 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 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 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 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 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 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 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 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 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 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.

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 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 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 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 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 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. 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 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 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 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 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 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 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 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 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.

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.

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 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 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 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.

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 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 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.

5 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.

10 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.

15 Referring to Fig. 6, the data updating method according to the present disclosure includes 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.

20 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 such 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.

25 After entering the operation mode from the heartbeat sleep mode, the smart cover sends the smart cover identification list 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 receiving an operation instruction input by the user
30 (such as an operation instruction input by the user by pressing a button). If the smart cover is used for the first time or has never successfully downloaded the smart cover identification list, the smart

cover does not store the smart cover identification list, and the smart cover conducts first processing to the default identification using the second secure transmission key and sends to the real card manager.

The real card manager receives the identification list of smart cover end sent by the smart cover, and 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. Specifically, if the real card manager receives the default identification, then determines that it is not the same.

If not the same, 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 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 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 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 smart cover sends the 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, such that 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 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, sending the default identification to the real card manager so that the real card manager issues a list of real card manager end and the real card information list of real card manager end to smart cover, wherein the default identification may be an empty identification, a predefined value, or a predefined character.

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

Or, 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 smart cover 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 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 smart cover, so that the smart cover directly issues the real card information list of smart cover end to the smart cover.

Certainly, after determining that an updating is required, the smart cover 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.

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 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 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 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 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 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.

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.

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.

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

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.

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.

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 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.

The present invention provides a concrete implementation of the mode one in the following:

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.

Referring to Fig. 7, the establishment of the secure connection between the smart cover and the simulation card includes followings.

The smart cover sends a first secure connection instruction for indicating the establishment of a secure connection to the simulation card, wherein the first secure connection instruction includes: encrypting a first binding factor as well as a first connection random factor to get a first connection ciphertext using public key of the simulation card in the certificate of a simulation card by the smart cover, signing a first binding factor as well as a first connection random factor to get a first connection signature message using private key of the smart cover; specifically, prior to using the smart cover to interact with the simulation card, it is optional to establish a secure connection between the smart cover and the simulation card to improve the security of subsequent data interactions. Wherein the first secure connection command for indicating the establishment of a secure connection may be generated for connection of a physical key provided separately on the ferrule or may be generated by connecting a virtual key on the touch screen of the smart cover, or may be generated after the activation password is verified correctly, or can be generated when the simulation card is pulled out of the smart cover, or can be generated for selecting the connection function in the menu displayed on the smart cover screen, or can be generated after the user chooses real card obtained for the smart cover real card information list. Of course, it can be generated in any other way, and is not limited in the present invention. Wherein the first connection random factor may be a random number, a random character, or a combination thereof generated by the smart cover, and of course, after generating the first connection random factor, the randomness of the first connection random factor may be verified to increase the randomness of the first connection random factor, and prevent from being cracked; specifically, the smart cover uses the simulation card public key to encrypt the first binding factor and the first connection random factor to ensure the security of the first binding factor and the first connection random factor transmission, the smart cover uses the smart cover's private key to sign the first binding

factor and the first connection random factor to ensure that the subsequent simulation card can authenticate the legitimacy of the card's identity. Sending the first binding factor of the cartridge to the simulation card so that the subsequent simulation card judges whether the first binding factor of the card is the same as the stored binding factor thereof to determine whether the card is tied to the simulation smart cover. Optionally, before this step, the smart cover detects the simulation card, the smart cover can determine whether the simulation card is in the first binding list of the cartridge, for example, it can be judged by the following: (the simulation card unique identification and / or simulation card certificate, etc.) is received by the simulation card after receiving the simulation card, and the simulation card is judged whether or not the simulation card is in the first binding list; and / or can also be determined by the simulation card whether the smart cover is in the simulation card end binding list. For example, the card can be used to determine whether the card information (such as the smart cover uniquely identifies and / smart cover certificate, etc.) sent to the simulation card, the simulation card based on the received smart covers of information to determine whether the card in the simulation card end of the binding list; only Perform a follow-up process after determines the other in their own binding list to optimize the process and improve efficiency.

The simulation card receives the first secure connection instruction, decrypts the first connection ciphertext using the private key of the simulation card to get the first binding factor and the first connection random factor; specifically, the first connection ciphertext is decrypted using the simulation card private key. If a data transmission error occurs during data transmission or tampering occurs during data transmission, it will result in failure to decrypt or decrypt the smart cover first binding decryption factor and the first connection random decryption factor are different from the first binding factor and the first connection random factor. And by simulating the card public key encryption, only the simulation card private key can be successfully decrypted, which can also guarantee the security of data decryption.

The simulation card verifies the first connection signature message using the public key of the smart cover in the certification of the smart cover, the first binding factor and the first connection random factor; specifically, the simulation card uses the cardholder's public key to verify the signature sent by the smart cover to ensure the legal source of the data.

The simulation card verification of one connection after the signature is correct, verify the ferrule end I bound to decrypt the same factor and a simulation card-binding factor; in particular,

the simulation card also verifies that the decrypted first-bound decryption factor is the same as the simulation card side binding factor stored by the simulation card itself, and if it is the same, it indicates that the card is securely connected to the simulation card before the binding operation has been completed, based on this, the simulation card can determine whether the card is bound with the simulation card.

The simulation card generates the second random factor after verifies that the first binding decryption factor is the same as the simulation card end binding factor; in particular, the second connection random factor may be a random number, a random character, or a combination thereof generated for the simulation card. Of course, after generating the second connection random factor, the randomness of the second connection random factor may also be verified to increase the randomness of the second connection random factor and prevent the crack.

The simulation card encrypts the first connection random decryption factor and the second connection random factor using the smart cover public key in the smart cover certificate to obtain the second connection ciphertext, uses the simulation card private key to sign the first connection random decryption factor and the second connection random factor to obtain a second connection signature; In particular, the simulation card encrypts the first connection random decryption factor and the second connection random factor using the smart cover public key to ensure the security of the first connection random decryption factor and the second connection random factor transmission, and the simulation card utilizes the simulation card private key to sign the first connection random decryption factor and the second connection random factor to ensure that the subsequent smart covers can authenticate the legitimacy of the simulation card identity.

The simulation card sends the response of a secure connection to the set of cards, in which, the secure connection response include: the second connection signature ciphertext and the second connection; specifically, the simulation card sends a second connection ciphertext and a second connection signature to the smart cover so that the card can decrypt and verify the received data.

The smart covers the first secure connection response, decrypts the second connection ciphertext with the key of the smart cover, obtains the decrypted first connection random decryption factor and the second connection random decryption factor; specifically, the second connection ciphertext is decrypted using the card private key, and if a data transmission error occurs during data transmission or tampering occurs in the data transmission, it will result in failure to decrypt successfully or decrypt the first connection random decryption factor and the

second connection random decryption factor are different from the first connection random factor and the second connection random factor. And through the smart cover public key encryption, only the card private key can be successfully decrypted, which can also guarantee the security of data decryption.

5 The smart cover verifies the second connection signature using the simulation card public key in the simulation card certificate, the decrypted first connection random decryption factor, and the second connection random decryption factor; in particular, The smart cover verifies the signature of the simulation card using the simulation card public key to verify the legal source of the data.

10 After confirming that the second connection signature is correct, verify that the first connection random decryption factor is the same as the first connection random factor; Specifically, the smart cover verifies that the first connection random factor generated by itself is the same as the decrypted first connection random decryption factor, which ensures that the data has not been tampered with, and the encrypted data source does send the first connection random factor object for the cartridge.

15 The first connection random decryption factor is decrypted and the first connection random factor is the same, and the first secure transmission key between the card and the simulation card is generated by using the second connection random decryption factor at least; the simulation card generates an simulation card-side secure transmission key between the smart cover and the simulation card using at least the second connection random factor. Specifically, the smart cover
20 can generate a first secure transmission key between the smart cover and the simulation card between the card and the card using the second connection random decryption factor, or use the first connection random factor, the second connection random decryption factor to generate the first secure transmission key between the smart cover and the simulation card, or the first secure transmission key can also be generated using the first connection random factor, the second
25 connection random decryption factor, and the first binding factor of the cartridge; similarly, the simulation card can also use the second connection random factor to generate an simulation card-side secure transport key between the smart cover and the simulation card, or use the first connection random decryption factor, the second connection random factor to generate an simulation card-side secure transmission key between the smart cover and the simulation card, it is
30 also possible to generate an simulation card-side secure transmission key between the smart cover and the simulation card using the first connection random decryption factor, the second connection

random factor, and the simulation card end binding factor; as long as the card and the simulation card using the same parameters of the same algorithm to generate a secure transmission key can be. It can thus be seen that in the present invention the secure transmission key factor may be a second connection random decryption factor, or a second connection random decryption factor and a first connection random factor at the cartridge end; the secure transmission key factor may be a second connection random factor on the simulation card, or a second connection random factor and a first connection random decryption factor. In addition, the secure transmission key may include encryption and decryption key and / or verification key, use encryption and decryption key can participate in the data transmission can guarantee the security of data transmission, use the verification key to participate in data transmission can guarantee the data transmission integrity, in the present invention, a secure transmission key may be selectively used according to the security level of the transmission data.

Of course, in the present invention, the step of generating an simulation card-side secure transmission key between the card and the simulation card using at least the second connection random factor in the present invention is not limited to the steps in the present embodiment, it is also possible to generate an simulation card-side secure transport key after the simulation card generates a second connection random factor, it can also generate the simulation card-side secure transmission key after receiving the success information sent by the packet holder after the first connection random decryption factor of the first connection is decrypted and the first connection random factor is the same.

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.

If the smart cover and the simulation card to establish a secure connection before the implementation of the manual binding and storage binding factor and other operations, in this way one, smart covers and simulation cards in addition to mutual authentication each other's identity, but also need to authenticate each other certificate.

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.

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 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 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.

The present invention provides a concrete implementation of the mode two in the following:

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.

Referring Fig. 8, establishing a secure connection between the smart cover and the simulation card includes:

The smart cover receives third random factors generated by simulation card and simulation card unique identification card sent by simulation card; in particular, the third connection random factor may be a random number, a random character, or a combination thereof generated for the simulation card, of course, after generating the third connection random factor, the randomness of the third connection random factor can also be verified to improve the randomness of the third connection random factor and prevent cracking. Prior to this step, the simulation card generates a third connection random factor, and after the smart covers the simulation card, the simulation card sends the third connection random factor and the simulation card unique identifier to the smart

cover.

The smart cover sends simulation card used to indicate the second secure connection instructions to establish a secure connection, wherein the second secure connection instruction comprises: a card uniquely identifying a third connection cipher obtained by encrypting the third connection random factor and the generated fourth connection random factor using the simulation card public key in the simulation card certificate, the third connection signature obtained by signing the third connection random factor and the fourth connection random factor using the smart cover private key; specifically, prior to using the smart cover to interact with the simulation card, it is optional to establish a secure connection between the smart cover and the simulation card to improve the security of subsequent data interactions. Wherein the second secure connection command for indicating the establishment of the secure connection may be generated for the connection physical key provided separately on the ferrule or may be generated by connecting the virtual key on the touch screen of the smart cover, or can be generated after the activation password is verified correctly, or can be generated when the simulation card is removed from the smart cover or can be selected for the menu displayed on the card screen, or can be in the smart cover to obtain the smart cover real card information list, the user from the choice of real card generated after. Of course, it can be generated in any other way, and is not limited in the present invention. In particular, the smart cover encrypts the third connection random factor and the generated fourth connection random factor using the simulation card public key to ensure the security of the third connection random factor and the generated fourth connection random factor transmission, The smart cover uses the smart cover private key to sign the third connection random factor and the generated fourth connection random factor to ensure that the subsequent simulation card can authenticate the legitimacy of the smart cover's identity. In addition, the fourth connection random factor may be a random number, a random character, or a combination thereof generated for the smart cover, of course, after generating the fourth connection random factor, it can also verify the randomness of the fourth connection random factor to improve the randomness of the fourth connection random factor to prevent cracking; optionally, before this step, the smart cover receives a unique identification of the simulation card, the card can be based on the unique identification of the simulation card to determine whether the simulation card in the first end of the card binding list, only after the judgment card is in the first binding list of the smart cover end, the subsequent process is performed to optimize the process and improve the efficiency.

The simulation card receives the second secure connection instruction to determine whether the smart cover uniquely identifies whether it is in the simulation card end binding list; specifically, the simulation card according to the received card unique identification to determine whether the card in the simulation card end of the binding list; only in the judgment smart cover in the simulation card end of the binding list, the implementation of the follow-up process, optimize the process and improve efficiency.

If the smart cover unique identification is in the simulation card end binding list, the simulation card decrypts the third connection cipher using the simulation card private key, obtains the third connection random decryption factor and the fourth connection random decryption factor; specifically, the third connection ciphertext is decrypted using the simulation card private key, and if a data transmission error occurs during data transmission or tampering occurs during data transmission, it will result in failure to decrypt successfully, or a third connection random decryption factor and the fourth connection random decryption factor are different from the third connection random factor and the fourth connection random factor. And encrypts with the simulation card public key, only the simulation card private key can be successfully decrypted, which can also guarantee the security of data decryption.

The simulation card uses the smart cover public key in the smart cover certificate, the third connection random decryption factor and the fourth connection random decryption factor to verify the third connection signature; specifically, the simulation card uses the smart cover's public key to verify the signature sent by the smart cover to ensure the legal source of the data.

After verifying that the third connection signature is correct, verify whether the third connection random decryption factor is the same as the third connection random factor; specifically, the simulation card verifies that the third connection random factor generated by itself is the same as the third connection random decryption factor, which ensures that the data has not been tampered with, and that the encrypted data source does send the object of the third connection random factor to the simulation card.

If the third connection random decryption factor is the same as the third connection random factor, the simulation card uses the simulation card private key to sign the fourth connection random decryption factor and the fourth connection random decryption factor to obtain the fourth connection signature; specifically, the simulation card uses the simulation card private key to sign the third connection random decryption factor and the fourth connection random decryption factor

to ensure that the subsequent smart covers can authenticate the legitimacy of the simulation card identity.

The simulation card sends a second secure connection response to the smart cover, wherein the second secure connection response comprises: a fourth connection signature; specifically, the simulation card sends a fourth connection signature to the smart cover so that the smart covers the received data for verification.

The smart cover receives the second secure connection response, verifies the fourth connection signature using the simulation card public key, the third connection random factor and the fourth connection random factor in the simulation card certificate; specifically, the smart cover verifies the signature of the simulation card using the simulation card public key to verify the legal source of the data.

The first secure transmission key is generated by using the fourth connection random factor and the first binding factor of the smart cover to generate the first secure transmission key between the smart cover and the simulation card; the simulation card generates the simulation card-side secure transmission key between the card and the simulation card using at least the fourth connection random decryption factor and the simulation card end binding factor; specifically, the smart cover can generate a first secure transmission key between the smart cover and the simulation card using first binding factor of the smart cover using the fourth connection random factor of the smart cover, the first secure transmission key can also be generated by using the third connection random factor, the fourth connection random factor, and the first binding factor of the cartridge to generate the smart cover between the card and the simulation card; similarly, the simulation card can also use the fourth connection random decryption factor and simulation card end binding factor to generate security transmission key between the smart cover and simulation card, or use the third connection random factor, the fourth connection random decryption factor and the simulation card end binding factor to generate the card and simulation card between the simulation card security transmission key; as long as the card and the simulation card using the same parameters of the same algorithm to generate a secure transmission key can be. Thus, in the present invention, the secure transmission key factor may be a fourth connection random factor, or a third connection random factor and a fourth connection random factor at the cartridge end; the secure transmission key factor may be a fourth connection random decryption factor on the simulation card, or a third connection random factor and a fourth connection random decryption

factor. In addition, the secure transmission key may include encryption and decryption key and / or verification key. The use of encryption and decryption key can participate in the data transmission can guarantee the security of data transmission, use the verification key to participate in data transmission can guarantee the data transmission Integrity, in the present invention, a secure transmission key may be selectively used according to the security level of the transmission data.

The smart cover sends the first connection random factor and the fourth connection random factor to the simulation card by using the first secure transmission key of the smart cover end; the simulation card sends the first connection random decryption factor and the fourth connection random decryption factor to the card case by using the simulation card side secure transmission key; specifically, the two parties use the respective secure transmission key to generate the first processing of the data and send it to the other party so that the other party verifies whether or not the secure transmission key generated by both parties is the same.

The smart cover receives the data sent by the simulation card and performs the second processing on the received data using the first secure transmission key of the smart cover to compare the second processed data with the third connection random factor and the fourth connection random factor the same; and the second processing is compared with the third connection random decryption factor and the fourth connection random decryption factor whether the data of the second processing is compared with the third connection random decryption factor the same. Specifically, the two parties perform the second processing on the received data using the respective secure transmission key generated, and each of them compares the data after the second processing with the respective data, If the same, then the two sides to generate the same security transmission key, in order to ensure that the two sides can use each of the subsequent generation of secure transmission key for data security transmission. In addition, while verifying that the two sides generate the same security transmission key, you can also verify that the binding factors are the same, and further verify that the other party is the real binding object, and further improve the security of subsequent data transmission.

Of course, in the present invention, the step of generating the simulation card-side secure transmission key by the simulation card is not limited to the steps in the second embodiment, it is also possible to generate an simulation card-side secure transmission key after decrypting the fourth connection random decryption factor, or after confirming that the fourth connection signature sent by the simulation card is correct, the successor information sent by the smart covers

is generated to generate the simulation card-side secure transmission key; the step of generating the first secure transmission key is not limited to the steps in the second embodiment, but also the first secure transmission key of the smart cover after the fourth connection random factor is generated by the smart cover.

Thus, based on the card and the simulation card to establish a secure connection, you can improve the security of data transmission, but also can verify whether the two sides were bound to further improve the security.

If the smart cover and the simulation card to establish a secure connection before the implementation of the manual binding and storage binding factor and other operations, then in the way two, smart covers and simulation cards in addition to mutual authentication of each other's identity, but also need to authenticate each other certificate.

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, 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 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 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 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.

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 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 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 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 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 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 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.

The following is a brief description of the smart cover with the real card manager using a way to establish a secure connection as follows, which is no longer detailed here.

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 connection may be realized via the data interaction method or the data interaction system.

Referring Fig. 9, establishing a secure connection between the smart cover and the simulation card includes following.

The smart cover to send to the real card manager a third secure connection instruction for indicating the establishment of a secure connection, wherein the third secure connection instruction comprises: a smart cover encrypting the fifth connection using the real card manager public key in the real card manager certificate to encrypt the second binding factor and the generated fifth connection random factor the second connection signature obtained by signing the second binding factor and the fifth connection random factor using the smart cover private key.

The real card manager receives the third secure connection instruction, decrypts the fifth connection cipher using the real card manager private key, obtains the second binding decryption factor and the fifth connection random decryption factor.

The real card manager validates the fifth connection signature using the smart cover public key, the second binding decryption factor and the fifth connection random decryption factor in the smart cover certificate; after the real card manager verifies that the fifth connection is correct, verify that the second binding decryption factor is the same as the true card manager binding factor.

The real card manager verifies that the second binding decryption factor is the same as the real card manager end binding factor, resulting in a sixth join random factor.

The real card manager obtains the sixth connection ciphertext by encrypting the fifth connection random decryption factor and the sixth connection random factor using the card public key in the smart cover certificate, and using the real card manager private key to the fifth connection random decryption factor and a sixth connection random factor to obtain a sixth connection signature; the real card manager sends a third secure connection response to the smart cover, wherein the third secure connection response comprises: a sixth connection ciphertext and a sixth connection signature.

The smart covers the third secure connection response, decrypts the sixth connection ciphertext with the card private key, obtains the decrypted fifth connection random decryption factor and the sixth connection random decryption factor.

5 The smart cover validates the sixth connection signature using the real card manager public key in the real card manager certificate, the decrypted fifth connection random decryption factor, and the sixth connection random decryption factor.

10 After confirming that the sixth connection signature is correct, verify that the fifth connection random decryption factor and the fifth connection random factor are the same; the fifth connection random decryption factor is decrypted and the fifth connection random factor is the same, and at least the sixth connection random decryption factor is used to generate the second secure transmission key between the smart cover and the real card manager; the real card manager uses at least the sixth connection random factor to generate a real card manager secure transport key between the smart cover and the real card manager.

15 Of course, in the present invention, the steps of the real card manager to generate the secure transfer key from the real card manager side using at least the sixth connection random factor generation card and the real card manager are not limited to the steps in the present mode one, it is also possible to generate a real card manager secure transport key after generating the sixth connection random factor in the real card manager, it can also generate the real card manager-side secure transmission key after receiving the success information sent by the card after the fifth connection random decryption factor of the fifth connection random decryption factor and the fifth connection random factor.

Thus, based on the card and the real card manager to establish a secure connection, you can improve the security of data transmission, but also can verify whether the two sides were bound to further improve the security.

25 If the smart cover and the real card manager to establish a secure connection before the implementation of the manual binding and storage binding factor and other operations, then in this way one, the card and the real card manager in addition to mutual authentication each other's identity, but also need to authenticate each other's certificate.

30 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, 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 function from a menu displayed on the screen of the smart

cover.

The following is a brief description of the smart cover with the real card manager using mode 2 to establish a secure connection as follows, and is not described here in detail.

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 system.

Referring Fig. 10, the smart cover with the real card manager to establish a secure connection includes following.

The card receives the real card manager to send the real card manager generated by the seventh connection random factor and the real card manager uniquely identifies.

A fourth secure connection instruction for indicating the establishment of a secure connection is sent to the real card manager by the smart cover, wherein the fourth secure connection instruction comprises: a card holder unique identifier, the card holder utilizes the real card manager public key in the real card manager certificate to the seventh connection random factor and the seventh connection ciphertext obtained by encrypting the generated eighth connection random factor, the second connection signature obtained by signing the seventh connection random factor and the eighth connection random factor with the card holder private key.

The real card manager receives the fourth secure connection command to determine whether the card holder uniquely identifies is in the real card manager side binding list.

If the card holder uniquely identifies is in the real card manager end binding list, the real card manager utilizes the real card manager private key decrypts the seventh connection ciphertext, obtains the seventh connection random decryption factor and the eighth connection random decryption factor.

The real card manager validates the seventh connection signature using the smart cover public key in the smart cover certificate, the seventh connection random decryption factor, and the eighth connection random decryption factor.

The real card manager verifies whether the random decryption factor is the same as the seventh connection random factor after verifies that the seventh connection signature is correct.

If the seventh connection random decryption factor is the same as the seventh connection random factor, the real card manager uses the real card manager private key to sign the seventh

connection random decryption factor and the eighth connection random decryption factor to obtain the eighth connection signature.

The real card manager sends a fourth secure connection response to the card holder, wherein the fourth secure connection response includes: the eighth connection signature.

5 The card holder receives the fourth secure connection response, uses the real card manager public key in the real card manager certificate, the seventh connection random factor and the eighth connection random factor to verify the eighth connection signature.

10 After confirming that the eighth connection signature is correct, at least the second connection random factor and the second binding factor of the card are used to generate the second secure transmission key between the card holder and the real card manager. The real card manager generates a real card manager secure transport key between the smart cover and the real card manager at least using the eighth connection random decryption factor and the real card manager end binding factor.

15 The card holder sends the seventh connection random factor and the eighth connection random factor to the real card manager after first processing using the second security transmission key; the real card manager sends the seventh connection random decryption factor and the eighth connection random decryption factor after first processing using the real card manager side secure transmission key.

20 The card receives the data sent by the real card manager and performs the second processing on the received data using the second secure transmission key of the card holder, compares whether the second processed data is the same as the seventh connection random factor and the eighth connection random factor; the real card manager receives the data sent by the card holder and uses the real card manager side secure transmission key to perform the second processing on the received data, compares the second processed data with the seventh connection random decryption factor and the eighth connection random decryption factor.

25 Thus, based on the card and the real card manager to establish a secure connection, you can improve the security of data transmission, but also can verify whether the two sides were bound to further improve the security.

30 Of course, in the present invention, the step of generating the real card manager side secure transmission key by the real card manager is not limited to the steps in the second embodiment, or in the decryption to obtain the eighth connection random decryption factor to generate a real card

manager-side security transmission key, or in the card to verify the real card manager to send the eighth connection signature is correct, after receiving the success of the packet sent to generate a real card manager-side secure transmission key; the step of generating the second secure transmission key of the smart cover is not limited to the steps in the second embodiment, and the second secure transmission key may be generated after the eighth connection random factor is generated by the card holder.

If the smart cover and the real card manager to establish a secure connection before the implementation of the manual binding and storage binding factor and other operations, then in the way two, the card and the real card manager in addition to mutual authentication each other's identity, but also need to authenticate each other's certificate.

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, 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 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 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.

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 the alarm password, the real card manager determines that the password to be verified passes verification, and performs an alarming operation. 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.

The following provides a way to achieve mode one:

The smart cover searches the smart cover identification list; specifically, the card-side identification list is a list of real card manager-side identities obtained from the real card manager for the smart cover.

If the smart cover finds the smart cover of identification list, sends the smart cover of identification list to the real card manager after first processing with the second security transmission key, the real card manager receives the data sent by the smart covers, performs a second processing to the received data using the real card manager side secure transmission key, judges whether the second processed data is the same as the real card manager side identification

list stored by the real card manager, if not, the real card manager performs the first processing to the update command and the update data using the real card manager secure transmission key and sends the processed data to the smart cover, the smart cover receives the data sent by the real card manager, performs the second processing to the received data using the second security transmission key, updates the real card information list in the smart cover end. Specifically, updating the real card information list in the smart cover end can be carried out as follows: The update instructions sent by the real card manager include adding and / or deleting instructions that include real card information that needs to be added or deleted, the smart covers, upon receiving the update instruction and updating the data, performs an addition and / or deletion operation on the smart cover real card information list according to the update instruction and the update data; or the update instructions sent by the real card manager include the addition and / or deletion of the instructions including the identification of the actual card information that needs to be added to the actual card information or to be deleted, after receiving the update instruction and updating the data, the smart covers the addition and / or deletion operation on the card's real card information list according to the update instruction and the update data; Alternatively, the update instructions sent by the real card manager include replacement instructions, including the latest real card manager real card information list, after receiving the update instruction and updating the data, the smart covers the replacement operation on the card's true card information list according to the update instruction and the update data.

20 If the smart cover does not find the smart cover identification list, the default identification is sent to the real card manager after performs the first processing using the second secure transmission key of the smart cover, the real card manager receives the data sent by the smart covers, performs the second processing to the received data using the real card manager side secure transmission key, if the real card manager determines that the second processed data is used to indicate that the smart cover side does not store the smart cover end identification list, sends the update instruction and the update data after first processing with the real card manager side secure transmission to the smart cover, the card receives the data sent by the real card manager, uses the second security transmission key of the card to performs the second processing on the received data, updates the smart cover real card information list. Specifically, the updated smart cover real card information list can be carried out by the following: The update instructions sent by the real card manager include storage instructions, including the latest real card manager real card

information list, after receiving the update command and update data, the smart covers the storage operation on the card's real card information list according to the update instruction and the update data.

Based on the above-mentioned realization scheme of the mode one, the smart covers are judged whether the smart cover's identity list is sent to the real card manager to judge whether the card number is too much smaller than the real card information list, as a result, the amount of data transferred data is reduced, the data transmission rate is increased, and the judgment rate of the real card manager is improved. If the smart cover is used for the first time, the smart cover itself does not store the smart cover end identification list, At this point, send the default logo to the real card manager so that the real card manager issues a real card manager side identification list and a real card manager real card information list to the smart cover, which can be empty, predefined values, or predefined characters.

Of course, the present invention is not limited to the above-described implementation of the first embodiment, and it is also possible to realize the updating of the card-type real card information list by one of the following ways when the smart cover and the real card manager do not store the identification list:

From the smart cover to the real card manager directly send the smart cover real card information list, so that the real card manager to compare after the judge whether to update; or

From the smart cover to the real card manager to send the list number of the real card information list of the smart cover so that the real card manager compares whether or not the list number is the same or not;

After receiving the user-entered update command from the real card manager, the real card manager sends the real card manager's real card information list to the smart cover.

Of course, in the real card manager to determine the need to update, you can also send an update request to the smart covers, smart covers that update the request to the user, so that the user to confirm whether to update.

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.

The real card manager using real card manager-side security transmission key to perform the first processing on the real card manager side identification list and sent to the smart cover;

The smart cover receives the data sent by the real card manager, uses the second secure transmission key of the smart cover to perform the second processing on the received data, determines whether the second processed data is the same as the smart cover identification list stored by the smart cover; specifically, if the smart cover is used for the first time or has never successfully downloaded the real card manager side identification list, the smart cover end identification list is not stored, and the judgment can be made directly.

If not, the smart cover sends the update request to the real card manager.

The real card manager receives the update request, uses the real card manager side security transmission key to perform the first processing to the update instruction and the update data, sends to the smart cover.

The card receives the data sent by the real card manager, uses the second security transmission key of the card to carry on the second processing to the received data, updates the smart cover real card information list. Specifically, updating smart cover real card information list can be carried out as follows: the update instructions sent by the real card manager include adding and / or deleting instructions that include real card information that needs to be added or deleted, after receiving the update instruction and updating the data, the smart covers the addition and / or deletion operation on the card's real card information list according to the update instruction and the update data; or the update instructions sent by the real card manager include the addition and / or deletion of the instructions including the need to add the actual card information or the corresponding identification of the actual card information to be deleted, after receiving the update instruction and updating the data, update and/or delete operations on the card's true card information list based on the update and update data; or the update instructions sent by the real card manager include replacement instructions, including the latest real card manager real card information list, after receiving the update instruction and updating the data, the smart covers the replacement operation on the card's true card information list according to the update instruction and the update data.

Based on the above-mentioned realization of the mode two, the real card manager judges whether or not the real card manager side identification list is sent to the smart cover for judgment, as the real card manager side of the list of data is much smaller than the real card manager real card information list, therefore, reduce the amount of data transmission data, improve the data transfer rate, but also improve the card to determine the rate. If the smart cover is used for the first

time, then the card itself does not store the smart cover side identification list, at this time, receive a real card manager issued a real card manager side of the identity list, send the update request directly so that the real card manager sends the real card manager to the real card information list to the smart cover.

5 Of course, the present invention is not limited to the above-described implementation of the second aspect, and it is also possible to realize the updating of the card-type real card information list by one of the following ways when the smart cover and the real card manager do not store the identification list:

By the real card manager directly to the smart cover to send a real card manager real card
10 information list, so that the card directly stored; or

The real card manager sends the list number of the real card manager's real card information list to the smart cover so that the smart covers are the same as whether or not the list number is the same or not.

After receiving the user input update instruction, the smart covers the update request to the
15 real card manager so that the real card manager sends the real card manager real card information list to the smart cover.

Of course, the smart covers to determine the need for updates, you can also prompt the user to confirm whether to update, and the user to confirm the update, the implementation of the follow-up update operation.

20 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
25 the user.

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
30 convenience.

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.

5 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.

10 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.

15 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.

20 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.

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

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

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, if the smart cover receives the response information within the second preset time and the response information further contains the update prompt information, the smart cover stores update prompt information; wherein the update prompt information for the

real card manager to prompt the card that the real card manager has the real card manager-side real card information list to update the prompt message.

After the smart cover enters the work mode from the heart sleep mode, the smart cover sends the update trigger request to the real card manager; specifically, the smart cover can enter the working mode from the heart sleep mode by the following way: the smart cover receives the update prompt information and automatically enters the work mode, or the smart covers the user input command (such as the user to enter the key input instructions, etc.), enter the work mode.

The real card manager receives the update trigger request, uses the real card manager side secure transmission key to carry on the first processing to the real card manager side identification list and sends to the smart cover.

The card receives the data sent by the real card manager, performs the second processing on the received data using the second secure transmission key, determines whether the second processed data is the same as the smart cover identification list stored in the smart cover; Specifically, if the smart cover is used for the first time or has never successfully downloaded the list of real card manager identifiers, the list of smart covers is not stored.

If not, the smart cover sends an update request to the real card manager.

The real card manager receives the update request, sends the data to the smart cover after first processing on the update instruction and the update data using the real card manager side secure transmission key.

The smart cover receives the data sent by the real card manager, and then uses the second secure transmission key of the card to perform the second processing on the received data, and then updates the real card information list. Specifically, the updated smart cover real card information list can be carried out by adding the update instructions sent by the real card manager to include and / or delete instructions including real card information that needs to be added or deleted, Updating the command and updating the data, performing an addition and / or deletion operation on the card's real card information list according to the update instruction and the update data; or the update command sent by the real card manager includes adding and / or deleting instructions, updating the data including the need Adding the actual card information or the corresponding identification of the actual card information to be deleted, after the receipt of the update instruction and the update data, performing the addition and / or deletion operation on the card's true card information list according to the update instruction and the update data; , The

update command sent by the real card manager includes a replacement instruction including the latest real card manager real card information list, after receiving the update instruction and updating the data, according to the update instruction and the update data, Real card information list is executed for Change operation.

5 Based on the above three implementations, the real card manager sends the real card manager side identification list to the smart cover to determine whether it is consistent, since the real card manager side identifier list data is much smaller than the real card manager real card information List, thus reducing the amount of data transmitted data, improve the data transfer rate, but also improve the card to determine the rate. If the smart cover is used for the first time, the smart cover
10 itself does not store a list of the end of the smart cover. At this point, when the real card manager receives the real card manager's identity list, it sends the update request for real card management Send a real card manager to the real card information list to the smart cover.

Of course, the present invention is not limited to the above-described implementation of the third embodiment, and it is also possible to realize the updating of the smart cover real card
15 information list by one of the following ways when the smart cover and the real card manager do not store the identification list:

By the real card manager directly to the smart cover to send a real card manager real card information list, so that the card directly stored; or

The real card manager sends the list number of the real card manager's real card information
20 list to the smart cover so that the smart covers are the same as whether or not the list number is the same or not.

After receiving the user input update instruction, the smart covers the update request to the real card manager so that the real card manager sends the real card manager real card information list to the smart cover.

25 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.

When the smart cover is in heartbeat sleep mode, if the card receives the response information within the second preset time and the response information further contains the update
30 prompt information, the smart cover stores update prompt information. Wherein the update prompt information for the real card manager to prompt the card that the real card manager has real card

manager-side real card information list update prompt

After the smart cover enters the work mode from the heart sleep mode, the smart cover uses the second security transmission key of the card to carry out the first processing to the smart cover end identification list and sends it to the real card manager; specifically, the smart cover can enter the working mode from the heart sleep mode by the following way: the smart cover receives the update prompt information and automatically enters the work mode, or the smart covers the user input command (such as the user to enter the key input instructions, etc.), enter the work mode. If the smart cover is used for the first time or has never successfully downloaded the real card manager side identification list, the smart cover does not store a list of smart covers, at this point, the smart cover uses the second secure transmission key of the card to perform the first processing on the default identity and sends it to the real card manager.

The real card manager receives the data sent by the smart cover, uses the real card manager side secure transmission key to carry out second processing on the received data, determines whether the second processed data is the same as the real card manager side identity list stored on the real card manager; specifically, the real card manager receives the preset identity and also determines that it is not the same.

If not, the real card manager uses the real card manager secure transmission key to perform the first processing on the update command and the update data, and then send it to the smart cover.

The smart cover receives the data sent by the real card manager, and then uses the second secure transmission key of the card to perform the second processing on the received data, updates the real card information list of the smart cover. Specifically, the updated smart cover real card information list can be carried out by adding the update instructions sent by the real card manager to include and / or delete instructions including real card information that needs to be added or deleted, Updating the command and updating the data, performing an addition and / or deletion operation on the card's real card information list according to the update instruction and the update data; or the update command sent by the real card manager includes adding and / or deleting instructions, updating the data including the need Adding the actual card information or the corresponding identification of the actual card information to be deleted, after the receipt of the update instruction and the update data, performing the addition and / or deletion operation on the card's true card information list according to the update instruction and the update data; , The

update command sent by the real card manager includes a replacement instruction including the latest real card manager real card information list, after receiving the update instruction and updating the data, according to the update instruction and the update data, Real card information list is executed for Change operation.

Based on the above-mentioned realization scheme of the fourth aspect, the smart covers are judged by sending the smart cover identification list to the real card manager to determine whether the data of the card end identification list is much smaller than the real card information list of the smart cover, The amount of data transmitted data, improve the data transfer rate, but also improve the real card manager to determine the rate. If the smart cover is used for the first time, the smart cover itself does not store a list of smart covers, and then sends the default logo to the real card manager so that the real card manager issues a list of real card manager side identifiers and The real card manager real card information list to the smart cover, which can be empty, pre-defined, or predefined characters.

Of course, the present invention is not limited to the above-described realization of the fourth aspect, and it is also possible to realize the updating of the card-type real card information list by one of the following ways when the smart cover and the real card manager do not store the identification list:

From the smart cover to the real card manager directly send the smart cover real card information list, so that the real card manager to compare after the judge whether to update; or

From the smart cover to the real card manager to send the list number of the real card information list of the smart cover so that the real card manager compares whether or not the list number is the same or not;

After receiving the user-entered update command from the real card manager, the real card manager sends the real card manager's real card information list to the smart cover.

Optionally, after the real card manager opens or closes the smart cover to access all or part of the real card in the important card area, the real card manager's real card information list is updated, so the real card The manager will send the card information to the smart cover to open the smart cover to use the full or partial real card in the important card area so that the card can update the smart cover's real card information list; or in the real card management Open or close the smart cover on the important card area of all or part of the real card to connect the use of authority, the trigger smart cover of real card information list update process, update the way you can refer to the

above one way and two ways to update, Not elaborate here.

VI. binding

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.

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.

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.

The following provides a specific implementation of the binding operation of the card and the analog card.

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.

Referring to Fig. 11, the binding operation of the card and the simulation card includes:

The smart cover receives a trigger command for indicating the binding with the simulation card. Specifically, before the use of the smart cover, you can first perform a boot operation on the smart cover, at this time, optional, the smart covers the user to enter the power-on password, and receive the user to enter the power-on password to verify the correct password entered by the user, In the verification of the user to enter the boot password is correct, the implementation of the boot operation, smart covers into the work mode. Before using the card to interact with the simulation card, it is optional to bind the card to the simulation card to improve the security of subsequent

data interactions. Wherein the trigger command received by the smart cover for indicating that the smart cover is bound to the simulation card may be generated for a binding physical key provided separately on the ferrule or may be a binding on the touch screen of the smart cover or can be generated after the activation password is verified correctly, or can be generated by inserting the simulation card into the smart cover, or by selecting the binding function for the menu displayed on the smart cover screen. Of course, can be generated in any other way, and is not limited in the present invention.

The smart cover sends the first binding instruction to the simulation card, wherein the first binding command includes: the first binding random factor generated by the smart cover, the smart cover certificate and the unique identifier of the smart cover; In particular, the staple can send a first binding instruction to the simulation card via a contact connection (via a contact interface), which can also be sent to the simulation card via a non-contact connection (via a contactless interface or a wireless interface) A binding instruction, the former can improve the binding security, which can improve the binding convenience. The first binding instruction carries the first binding random factor to prevent the replay attack, the first binding instruction carries the staple certificate in order to simulate the card to authenticate the smart cover, the first binding instruction carries the smart cover uniquely Where the first binding random factor can generate a random number, a random character, or a combination of it, and, of course, after generating the first binding random factor, it is also possible to determine whether the first binding random number, The randomness of the binding random factor is verified to improve the randomness of the first binding random factor to prevent cracking; the smart cover unique identification may be any one of the smart cover serial number, the device identification code, the MAC address, or the like Unique identification of the identification of the card.

The simulation card receives the first binding instruction, uses the root certificate to verify the smart cover certificate. Specifically, the simulation card pre-stored the root certificate, the use of the root certificate to complete the verification of the certificate to ensure the follow-up use of the security of the certificate.

After the simulation card validates the smart cover certificate, the second binding random factor is generated; In particular, the second binding random factor may be a random number, a random character, or a combination thereof generated for the simulation card; of course, after generating the second bound random factor, it is also possible to verify the randomness of the

second bound random factor , To improve the randomness of the second binding random factor, to prevent being cracked.

The simulation card encrypts the first binding random factor and the second binding random factor to obtain the first binding ciphertext, signatures the first binding random factor and the second binding random factor to obtain the first binding signature. In particular, the simulation card encrypts the first binding random factor and the second binding random factor using the smart cover public key to ensure the security of the first binding random factor and the second binding random factor transmission, the simulation card utilizing the simulation card private key signs the first binding random factor and the second binding random factor to ensure that subsequent smart covers can authenticate the legitimacy of the simulation card identity

The simulation card sends the first binding response to the simulation card, wherein the first binding response includes a first binding cipher, a first binding signature, an simulation card certificate, and an simulation card unique identifier. In particular, the first binding response sent by the simulation card carries an simulation card certificate for the card to authenticate the simulation card, the first binding response carrying the unique identifier of the simulation card so that the card is informed which simulation card is bound to it; The simulation card unique identification may identify the identification of the card for any of the simulation card serial number, device identification code, MAC address, or any combination thereof.

The smart cover receives the first binding response, verifies the simulation card certificate with the root certificate. Specifically, the smart covers the root certificate in advance, using the root certificate to complete the verification of the simulation card certificate to ensure the follow-up use of simulation card certificate security.

After the verification of the simulation card certificate, the first binding ciphertext is decrypted by the smart cover private key, to obtain the first binding random decryption factor and the second binding random decryption factor. Specifically, the first binding ciphertext is decrypted using the card private key, and if a data transmission error occurs during data transmission or tampering occurs during data transmission, it will result in failure to decrypt successfully or decrypt the first binding random decryption factor and a second binding random decryption factor are different from the first bound random factor and the second bound random factor. And through the smart cover public key to encrypt, only the card private key can be successfully decrypted, which can also guarantee the security of data decryption.

The smart cover verifies the first binding signature using the simulation card public key in the simulation card certificate, the first binding random decryption factor and the second binding random decryption factor. Specifically, the smart cover validates the signature sent by the simulation card using the simulation card public key after verification to ensure that the legal source of the data

The smart cover verifies that the first binding random decryption factor is the same as the first binding random factor after confirming that the first binding signature is correct. Specifically, the card proves that the first binding random factor generated by itself is the same as the first binding random decryption factor, which ensures that the data has not been tampered with and that the encrypted data source does send the first binding random factor for the packet object.

If the first binding random decryption factor is the same as the first binding random factor, indicating the simulation card unique identification by the smart cover. Specifically, the smart cover can display a unique identifier for the simulation card, or it can be uniquely identified by voice playback (such as speaker playback or headphone playback, etc.) to allow the user to verify the authenticity of the simulation card and improve the binding security.

The smart cover receives the triggering command for confirming the simulation card unique identification is correct, signs the first binding random factor and the second binding random decryption factor with the smart cover private key to obtain the second binding signature, and stores the simulation card unique identification, the simulation card certificate and the first binding factor of the smart cover to the first binding list of the smart cover, wherein the first binding factor of the smart cover is the second binding random decryption factor; Specifically, the trigger command received by the smart cover for confirming that the simulation card is uniquely identified can be generated for confirmation of a physical key set on the smart cover alone or may be generated by a confirmation virtual key on the touch screen of the smart cover, or Select a confirmation function generated in the menu displayed on the smart cover screen or select a voice acknowledgment indication that can be received by the voice collection device (for example, Mike) of the smart cover and verify that it is generated after the pass, or can be collected for the fingerprint The device receives a fingerprint confirmation indication and verifies that the generated, or can be, the iris acquisition device for the smart cover receives the iris confirmation indication and validates it after passing it, and of course, it can also be generated for any other way in the present invention The first binding random factor and the second binding random decryption factor

are signed so that the subsequent simulation card can authenticate the identity of the smart cover. Of course, the smart cover can also store the first tie A list of the first binding list used to record information about the simulation card bound to the card, for example, Simulation card unique identification, simulation card certificate, etc. In addition, the first set of the first binding set is also
5 used to store the first binding factor, the first set of the first binding factor for the cube transmission of the second tie The stochastic factor based on the second binding random factor is transmitted in ciphertext, so the first binding factor of the card is safe and not tampered with.

The smart cover sends the second binding signature to the simulation card; Specifically, the smart covers a second binding signature to the simulation card to emulate the card to authenticate
10 the smart cover.

The simulation card receives the second binding signature, utilizes the smart cover public key in the smart cover certificate, the first binding random factor, and the second binding random factor to verify the second binding signature; Specifically, the simulation card validates the signature sent by the smart cover using the card key of the card after verification to ensure the
15 legal source of the data.

The simulation card verifies that the second binding signature is correct, stores the smart cover unique identification, the smart cover certificate, and the simulation card end binding factor to the simulation card end binding list, wherein the simulation card end binding factor is the second binding random factor. Specifically, the simulation card can also store a list of simulation
20 card end bindings that are used to record information about the smart cover that is bound to the simulation card, such as a card's unique identification, a set of certificates, and so on , the simulation card end binding list is also used to store the simulation card end binding factor, which is the second binding random factor generated by the simulation card.

It can be seen that, based on the above operation for binding the smart cover and the
25 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
30 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.

The following provides a specific implementation to perform a binding operation of the smart cover and the real card manager.

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 or the data interaction system.

Referring Fig. 12, the binding operation performed by the smart cover with the real card manager includes:

The smart cover receives the trigger command for indicating the binding with the real card manager. Specifically, before the use of the smart cover, you can first perform a boot operation on the smart cover, at this time, optional, the smart covers the user to enter the power-on password, and receive the user to enter the power-on password to verify the correct password entered by the user, In the verification of the user to enter the boot password is correct, the implementation of the boot operation, smart covers into the work mode. Before using the card to interact with the real card manager, it is optional to bind the smart cover to the real card manager to improve the security of subsequent data interactions. Wherein the trigger command received by the smart cover for indicating that the smart cover is bound to the real card manager may be generated for a binding physical key provided separately on the smart cover or may be bound on the touch screen

of the smart cover virtual keys generated, or can be generated after the activation password is verified correctly, or can be generated for selecting the binding function in the menu displayed on the smart cover screen. Of course, it can also be generated for any other way in the present invention without limitation.

5 The smart cover sends the second binding instruction to the real card manager over the wireless network, wherein the second binding instruction comprises: a third binding random factor generated by the smart cover, the smart cover certificate, and a smart cover unique identification; Specifically, the smart cover may send a second binding instruction to the real card manager via wireless means (e.g., mobile network, WIFI, etc.). The second binding instruction carries the third
10 binding random factor to prevent the replay attack, the second binding instruction carries the smart cover certificate so that the real card manager authenticates the smart cover, and the second binding instruction carries the only one where the third binding random factor can generate random numbers, random characters, or combinations thereof for the smart cover, and, of course, after generating the third binding random factor, it is also validated by the real card manager to
15 know which smart covers are bound to it; The randomness of the third binding random factor can be verified to improve the randomness of the third binding random factor to prevent being cracked; the unique identifier of the card can be any one such as the card serial number, the device identification code, the MAC address, etc. or a combination thereof to uniquely identify the identification of the smart cover.

20 The real card manager receives the second binding instruction and verifies the smart cover certificate with the root certificate. Specifically, the real card manager pre-stores the root certificate, using the root certificate to complete the verification of the card certificate to ensure the subsequent use of the security of the certificate.

 The real card manager generates the fourth binding random factor after verifies that the
25 certificate is legal. Specifically, the fourth binding random factor may be a random number, a random character, or a combination thereof generated by the real card manager; of course, after generating the fourth bound random factor, the randomness of the fourth bound random factor to verify the randomness of the fourth binding random factor to prevent being cracked.

 The real card manager encrypts the third binding random factor and the fourth bound random
30 factor using the smart cover public key in the smart cover certificate to obtain the second binding ciphertext, sign the third binding random factor and the fourth binding random factor using the real

card manager private key to obtain the third binding signature. Specifically, the real card manager encrypts the third binding random factor and the fourth binding random factor using the card public key to ensure that the third binding random factor and the fourth binding random factor transmission security, the real card manager uses the real card manager private key to sign the third binding random factor and the fourth binding random factor to ensure that subsequent smart covers can authenticate the legitimacy of the real card manager identity.

The real card manager sends a second binding response to the smart cover via the wireless network, Wherein the second binding response includes a second binding ciphertext, a third binding signature, a real card manager certificate, and a real card manager unique identification. Specifically, the second card response sent by the real card manager carries the real card manager certificate so that the smart cover authenticates the real card manager, and the second binding response carries the unique identity of the real card manager so that the packet is informed of which real card manager is uniquely identified as a real card manager serial number, device identification code, MAC address, etc., or any combination thereof to uniquely identify the identity of the real card manager.

The smart cover receives the second binding response and verifies the real card manager certificate using the root certificate. Specifically, the smart cover pre-stores the root certificate, using the root certificate to complete the verification of the real card manager certificate to ensure the subsequent use of real card manager certificate security.

After confirming that the real card manager certificate is valid, the second binding ciphertext is decrypted by the card private key to obtain the third binding random decryption factor and the fourth binding random decryption factor, specifically, the second binding ciphertext is decrypted using the packet private key, and if a data transmission error occurs during data transmission or tampering occurs during data transmission, it will result in failure to decrypt successfully or decrypt the second Three binding random decryption factors and the fourth binding random decryption factor are different from the third binding random factor and the fourth binding random factor. And through the smart cover public key to encrypt, only the card private key can be successfully decrypted, which can also guarantee the security of data decryption

The smart cover verifies the third binding signature using the real card manager public key in the real card manager certificate, the third binding random decryption factor, and the fourth binding random decryption factor. Specifically, the smart cover validates the signature sent by the

real card manager using the real card manager public key after verification to ensure that the data is legitimate.

After verifying that the third binding is correct, the smart cover verifies whether the third binding random decryption factor is the same as the third binding random factor. Specifically, the smart covers itself to generate a third binding random factor that is the same as the third binding random decryption factor, which ensures that the data has not been tampered with and that the encrypted data source does send a third binding random factor for the packet object.

The smart cover prompts the real card manager unique identification after verifies that the third binding random decryption factor is the same as the third binding random factor. Specifically, the smart cover can display the unique identity of the real card manager, or it can be uniquely identified by the real card manager for voice playback (such as speaker playback or by headset handset playback) so that the user can confirm the authenticity of the real card manager binding security.

The smart cover receives a trigger command used to confirm that the real card manager unique identification, sign the third binding random factor and the fourth binding random decryption factor with the smart cover private key, obtains the fourth binding signature, and stores the real card manager unique identification, the real card manager certificate and the second binding factor of the smart cover to the second binding list of the smart cover, wherein the second binding factor of the card is the fourth binding random decryption factor. Specifically, the trigger command received by the smart cover for confirming that the actual card manager is uniquely identified can be generated for confirmation of a physical key set on the smart cover alone or may be generated by a confirmation button on the touch screen of the smart cover , Or select a confirmation function generated in the menu displayed on the smart cover screen, or a voice confirmation indication received by a voice collection device (such as a microphone) for a smart cover and verify that it is generated after it is passed, The fingerprint collection device receives the fingerprint confirmation indication and verifies the generated or succeeded iris confirmation instruction and can be generated by the iris collection device which can be generated for the smart cover, and may otherwise be generated in any other way. In the present invention The use of the smart cover the private key to the third binding random factor and the fourth binding random decryption factor to sign in order to follow the real card manager to verify the identity of the smart cover; of course, the card can also store the smart cover The second binding list, which is the

second binding list used to record the actual card management with the card binding Related information, such as: real card manager unique identification, real card manager certificate, etc., in addition, the second end of the second set of bundled list is also used to store the second binding factor, The fourth bound random factor based on the fourth binding random factor is ciphertext transmission, so the second binding factor of the card is safe and not tampered with.

The smart cover sends the fourth binding signature to the real card manager. Specifically, the smart covers the fourth binding signature to the real card manager so that the real card manager authenticates the smart cover.

The real card manager receives the fourth binding signature, verifies the fourth binding signature using the smart cover public key in the smart cover certificate, the third binding random factor and the fourth binding random factor. Specifically, the real card manager verifies the signature sent by the smart cover using the card's public key after verification to ensure the legal source of the data.

After the real card manager verifies the four binding signature is correct, stores the smart cover unique identification, the smart cover certificate, and the real card manager binding factor to the real card manager side binding list, wherein the real card manager side binding factor is the fourth binding random factor. Specifically, the real card manager can also store a list of real card manager end bindings that are used to record information about the card bound to the real card manager, for example: Identity card manager certificate, etc., in addition, the real card manager side binding list is also used to store the real card manager end binding factor, the real card manager side binding factor for the real card manager generated fourth binding Random factor.

Thus, based on the card and the real card manager to bind, you can guarantee the follow-up card and the real card manager data exchange between the security.

In addition, the above card and the real card manager to perform the binding operation is not a necessary step, according to the needs of different application scenarios, you can choose not to implement the card and the real card manager to perform binding operations.

Of course, the above-mentioned card and the actual card manager to perform binding operations, is not limited to the implementation of the above provided, for example, you can also use manual binding, that is, in a trusted environment, The real card manager's identity is used as the first card binding factor, the real card manager defaults to the real card manager's identity as the real card manager binding factor; or the actual card manager enters the card to be bound Set

the identity of the card as a real card manager binding factor, the smart cover the default smart cover as the second end of the card binding factor; or in the smart cover to enter any random value as the second binding factor, The same random value is entered as the real card manager binding factor on the real card manager, etc., as long as the same binding factor can be obtained from the smart cover and the real card manager, all of which are within the scope of the present invention.

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 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 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 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.

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 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. 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 manager sends the data to be processed to the selected real card, such that the selected real card processes the data to be processed.

5 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 carrying real cards, thus improving convenience and security.

10 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.

15 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 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

20 With the data interaction architecture according to the present disclosure, 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.

25 In the following, a specific flow for recharging is provided, but the present is not 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 smart cover may be executed, which is no longer
30 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 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, 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 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 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. 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 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 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 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 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, 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.

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, 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 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.

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 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 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 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 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 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 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 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 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 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 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 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.

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 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 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.

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 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 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.

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.

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.

Referring to Fig. 13, updating an application of the smart cover includes:

The smart cover sends at least the smart cover certificate to a update platform. Specifically, a

secure update platform is set up separately to complete the update of the card application. The smart covers the smart covers to the update platform so that the update platform knows which smart covers need to be updated and can also verify the identity of the smart cover. The card can also update the application ID or other update platform that needs to be updated or the downloaded application's information is sent to the update platform so that the update platform knows which application package to send to the package.

The update platform generates the first update encryption key; specifically, the update platform itself generates an update encryption key for encrypting the application installation package, and the update encryption key generated each time the application update is performed may be the same or different, and the difference can be prevented from being cracked and the security is improved.

The update platform encrypts the smart cover installation package with the first update encryption key to obtain the first installation package ciphertext; specifically, the update platform encrypts the packet application installation package with the generated update encryption key to ensure the security of the packet application installation package transmission

The update platform uses the update platform private key to sign the first installation package to obtain the first installation package signature; specifically, the update platform signs the first installation package ciphertext so that the subsequent smart covers verify the identity of the update platform.

The update platform encrypts the first update encryption key using the smart cover public key in the smart cover certificate to obtain the first update encryption key ciphertext; specifically, the update platform updates the encryption key with the card public key encryption to ensure the security of the encryption key transmission. At the same time, it is guaranteed that only the card can decrypt the update encryption key and improve the security of the application installation package.

The update platform sends the smart cover update information to the smart cover, wherein the card update information includes: update the platform certificate, the first installation package ciphertext, the first installation package signature, and the first update encryption key ciphertext; specifically, the update information transmitted by the update platform carries the update platform certificate so that the smart cover authenticates the update platform, and the update information carries the first installation package ciphertext to ensure the security of the application installation

package transmission, and the update information carries the first installation packet signature to ensure that subsequent smart covers can update the identity of the identity of the platform to authenticate, update the information carried in the updated encryption key ciphertext to ensure the security of encryption key transmission.

5 The smart cover receives smart cover update information, use the root certificate to verify the update platform certificate; specifically, the smart cover pre-stores the root certificate, using the root certificate to complete the verification of the updated platform certificate to ensure the follow-up use of the update platform certificate security

10 After confirming the update platform certificate, the first installation package signature is checked by using the update platform public key in the update platform certificate; specifically, the smart cover verifies the signature sent by the update platform using the update platform public key in the updated platform certificate after verification to ensure that the legal source of the data.

15 After confirming that the first installation package signature is correct by the smart cover, the first encryption key is decrypted by the card private key to obtain the first decryption key. Specifically, the smart cover decrypts the decryption key with the card private key for subsequent decryption of the installation ciphertext to obtain the card package application package.

 The smart cover decrypts the first installation package using the first decryption key to obtain the package application package.

20 The smart cover verifies whether the data format of the package installation package is correct. Specifically, the smart covers also verify that the data format of the package application package is correct. If the data format of the package application package is not correct, the installation operation will not be performed. If the data format of the package application package is correct, performs the installation.

25 If so, the smart cover installs according to the application package. Specifically, if the card is updated for an installed application, it can overwrite the installed application, either upgrade the installed application, or uninstall the installed application before proceeding with the new application program installation, if the card is a new installation of the application, you can install the application directly.

30 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.

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.

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.

Referring to Fig. 14, updating an application of the smart cover includes:

The smart cover obtains the simulation card certificate from the simulation card, sends at least the simulation card certificate to the update platform. Specifically, the smart cover can obtain an simulation card certificate from the simulation card by sending a simulation card to the simulation card via a contact or non-contact, and sending a request to obtain an simulation card certificate, the simulation card receiving the card After sending the request, the simulation card certificate is sent to the smart cover, or the smart covers the simulation card to send the simulation card certificate to the smart cover after the card is detected by contact or non-contact. Alternative Alternatives: Once the card is detected by contact or non-contact, the simulation card is sent to the simulation card to obtain a request for a unique identification of the simulation card. After the card receives the request sent by the card, the simulation card will be sent To the smart cover, the smart cover to receive the unique identification of the simulation card can also be based on the unique identification of the simulation card from the local storage of the first set of bundled list of simulation cards to obtain a unique identification of the corresponding simulation card certificate; or smart covers through contact Type or non-contact detection of the simulation card, the simulation card will automatically emulate the unique identifier of the simulation card to the smart cover, the smart cover can receive a unique identification of the simulation card after the card can also be based on the unique identification of the card from the local storage of the first In the binding list, obtain an simulation card that uniquely identifies the corresponding simulation card certificate. In addition, a separate security update platform is set up to complete the update of the simulation card application. The smart covers the simulation card certificate to the update platform

so that the update platform knows which simulation card needs to be updated and also verifies the identity of the simulation card; the card can also update the application logo or other update platform that needs to be updated or The downloaded application's information is sent to the update platform so that the update platform knows which application package to send to the simulation card.

The update platform generates the second update encryption key. Specifically, the update platform itself generates an update encryption key for encrypting the application installation package, and the update encryption key generated each time the application update is performed may be the same or different, and the difference can be prevented from being cracked and the security is improved.

The update platform encrypts the simulation card application installation package with the second update encryption key to obtain the second installation package ciphertext. Specifically, the update platform encrypts the simulation card application installation package with the generated update encryption key to ensure the security of the simulation card application installation package transmission

The update platform uses the update platform private key to sign the second installation package to obtain the second installation package signature. Specifically, the update platform signs the second installation ciphertext so that the subsequent simulation card verifies the identity of the update platform.

The update platform encrypts the second update encryption key using the simulation card public key in the simulation card certificate to obtain the second update encryption key ciphertext. Specifically, the update platform uses the simulation card public key encryption update encryption key, can guarantee the update encryption key transmission security, at the same time, only to ensure that only the simulation card can decrypt the update encryption key, improve the security of the application installation package.

The update platform sends the simulation card update information to the smart cover, wherein the simulation card update information includes: updating the platform certificate, the second installation package ciphertext, the second installation package signature, and the second update encryption key ciphertext;

The smart cover receives the simulation card update information and sends it to the simulation card. Specifically, the update information sent by the update platform carries the update

platform certificate to simulate the card to authenticate the update platform, and the update information carries the second installation package to ensure the security of the application installation package transmission, and the update information carries the second installation packet signature to ensure that the subsequent simulation card can update the identity of the identity of the platform to authenticate, update the information to carry the updated encryption key ciphertext to ensure the security of encryption key transmission. Specifically, the smart cover uses the secure transmission key generated when the secure connection between the smart cover and the simulation card establishes the transmission of the simulation card update information, and can improve the security of the data transmission

The simulation card receives the simulation card update information sent by the smart cover, uses the root certificate to verify the update platform certificate. Specifically, the simulation card pre-stored the root certificate, the use of the root certificate to complete the verification of the updated platform certificate to ensure the follow-up use of the updated platform certificate security.

After the simulation card verifies the update platform certificate, uses the update platform public key in the update platform certificate to verify the second installation package signature. Specifically, the simulation card validates the signature sent by the update platform using the updated platform public key in the updated platform certificate after verification to ensure the legal source of the data.

After the simulation card verifies that the second installation package signature is correct, decrypts the second update encryption key ciphertext using the simulation card private key to obtain the second decryption key. Specifically, the simulation card decrypts the decryption key using the simulation card private key for subsequent decryption of the installation ciphertext to obtain an simulation card application installation package.

The simulation card decrypts the second installation package cipher using the second decryption key to obtain the simulation card application installation package.

Simulation card verifies whether the data format of the card application installation package is correct; Specifically, the simulation card also verifies that the data format of the simulation card application installation package is correct. If the data format of the simulation card application installation package is not correct, the installation operation is not performed. If the data format of the simulation card application installation package is correct, performed The installation.

If the simulation card verifies that the data for the format of the simulation card application installation package correctly, the simulation card is installed according to the simulation card application installation package. Specifically, if the demo card is updated for an installed application, you can overwrite the installed application, either upgrade the installed application, or
5 uninstall the installed application before proceeding with the new application program installation, if the simulation card is a new installation application, you can install the application directly.

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 downloaded and installed, thus extending functions of the simulation card, and making it convenient for the user to
10 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 performs the application updating.

15 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.

A specific implementation for updating the application of the real card manager is provided in
20 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.

Referring to Fig. 15, updating an application of the smart cover includes:

25 The real card manager sends at least the real card manager certificate to the update platform. Specifically, a secure update platform is set up separately to complete the update of the real card manager application. The real card manager sends the real card manager certificate to the update platform so that the update platform knows which real card manager needs to be updated and also verifies the identity of the real card manager; the real card manager can also update the application
30 that needs to be updated program logo or other information that prompts the update platform that the updated or downloaded application is sent to the update platform so that the update platform

knows which application installation package to send to the real card manager.

The update platform generates the third update encryption key. Specifically, the update platform itself generates an update encryption key for encrypting the application installation package, and the update encryption key generated each time the application update is performed
5 may be the same or different, and the difference can be prevented from being cracked and the security is improved.

The update platform utilizes the third update encryption key to the real card manager application installation package for encryption to obtain the third installation package. Specifically, the update platform encrypts the real card manager application installation package with the
10 generated update encryption key to ensure the security of the real card manager application installation package.

The update platform uses the update platform private key to sign the third installation package to obtain the third installation package signature. Specifically, the update platform signs the third installation ciphertext so that the subsequent real card manager verifies the identity of the
15 update platform.

The update platform using the real card manager certificate in the real card manager to obtain the third update encryption key. Specifically, the update platform uses the real card manager public key encryption to update the encryption key, can guarantee the update encryption key transmission security, at the same time, ensure that only the real card manager can decrypt the update
20 encryption key, improve the application installation packet transmission security.

The update platform sends the real card manager update information to the real card manager, wherein the real card manager update information includes: updating the platform certificate, the third installation package ciphertext, third install package signature and third update encryption key cipher text. Specifically, the updated platform sends the update information to carry the update
25 platform certificate so that the real card manager authenticates the update platform, and the update information carries the third installation package to ensure the security of the application installation package transmission, update the information to carry the third installation package signature to ensure that the follow-up real card manager can update the identity of the identity of the platform to authenticate, update the information to carry the updated encryption key ciphertext
30 to ensure the security of encryption key transmission.

The real card manager receives real card manager update information, uses root certificate to

verify update platform certificate. Specifically, the real card manager pre-stores the root certificate, the use of the root certificate to complete the verification of the updated platform certificate to ensure the follow-up use of the updated platform certificate security.

5 After the real card manager verifies the update platform certificate, the third installation package signature is checked by using the update platform public key in the update platform certificate. Specifically, the real card manager uses the update platform in the update platform certificate after verification The public key verifies the signature sent by the update platform to ensure the legal source of the data.

10 The real card manager verifies that the third installment package is correct and decrypts the third update encryption key using the real card manager private key to obtain the third decryption key; in particular, the real card manager utilizes the real card manager private The key decrypts the decryption key so that the subsequent decryption installs the ciphertext to obtain the real card manager application installation package.

15 The real card manager decrypts the third installation package using the third decryption key to obtain the real card manager application installation package;

The real card manager verifies that the real card manager application installs the package's data format is correct; specifically, the real card manager also verifies that the real card manager application installs the data format of the package if the real card manager application installs If the data format of the package is not correct, the installation operation is not performed if the data
20 format of the real card manager application installation package is correct.

If the real card manager verifies that the actual card manager application installation package has the correct data format, the real card manager is installed according to the real card manager application installation package. Specifically, if the real card manager updates an installed application, it can overwrite the installed application, either upgrade the installed application, or
25 uninstall the installed application before proceeding with the new application. Of the application installation, if the real card manager is a new installation application, you can install the application directly.

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
30 installed, thus extending functions of the real card manager, and making it convenient for the user's usage.

XI. data interaction architecture applicable scenario

1. recharging the account:

In an application scenario provided by the present embodiment, the user can realize the recharge of the third party account based on the above data interaction architecture, for example, to charge the Alipay account.

The implementation of this application scenario will be described in detail below, but the present invention is not limited thereto:

The smart covers the account platform through the network; in particular, the smart covers the account platform through the wireless network so that the recharge of the account is completed by the smart cover and the real card manager in the data interchange architecture of the present invention. Among them, the account platform can be a virtual third-party account platform, such as: e-commerce website account platform (such as Alipay, etc.), electricity payment platform, network financial platform (such as funds, etc.).

The card request sends the recharge request to the account platform, wherein the recharge request includes: the charge information; in particular, the smart covers the recharge request to the account platform so that the account platform can feedback the prepaid package according to the recharge request. Among them, the recharge information includes: the amount of recharge, etc., optional, you can also include the account to be recharged so that the account platform to know which account to recharge.

Wherein the prepaid package is generated by the payment platform upon receipt of the recharging request; in particular, the smart covers the recharging request to the payment platform after sending the refill request to the account platform at the same time or again, Or, the account platform to receive a recharge request, the recharge request sent to the payment platform to pay the platform will be paid. The payment platform to receive the recharge request, but also generate a recharge package, which includes: recharge the amount, to be recharge account and other information, the payment platform will be sent to the card pack, or payment platform will be sent to the account platform, And then by the account platform will be sent to the card pack, so that the user on the card to confirm the recharge package is correct. Among them, the payment platform for the real card corresponding to the trading platform, such as online banking and so on.

The smart covers the recharge card to receive the recharge pack, and then the card is displayed or the voice is played back so that the user can confirm the information in the prepaid

package, If the user confirms, confirm the operation on the smart cover (for example, press the confirmation button, select the confirmation option in the menu, etc.) to generate a confirmation command for confirming the correctness of the recharge pack. The smart covers the confirmation command so that the smart cover continues the follow-up operation; of course, if the user to
5 confirm the recharge package has a problem, you can cancel the operation on the card in order to cancel the pen recharge. The confirmation command received by the smart cover for confirming the correctness of the charge pack can be generated for the confirmation of the physical key set on the smart cover alone or by the confirmation of the virtual key on the touch panel of the smart cover, or on the smart cover screen (Or microphone) received by the voice collection device (for
10 example, Mike) received by the confirmation function in the displayed menu, or the fingerprint confirmation device that can be generated after the pass through, or can receive the fingerprint confirmation It is not possible to limit the use of the iris confirmation indication and the generation of the iris confirmation instruction and the verification of the pass generated by the iris acquisition device which can be generated and verified, or may be generated for any other means. Of course, .
15 at the same time as this step or before this step, the smart cover also needs to log in to the real card manager and select the real card for the account to recharge, the operation of the smart cover login real card manager and the operation of selecting the real card The above description is not described here in detail.

The card is sent to the real card manager by first processing the recharging packet using the
20 second secure transmission key of the smart cover, wherein the second secure transmission key is a secure connection between the smart cover and the real card manager Generated, the real card manager is connected to at least one real card and stores a real card manager real card information list, the real card manager real card information list includes a real card with a real card manager connected to the real card Information; in particular, the smart cover to receive the recharge
25 package, and in the recharge package confirmed correct, the prepaid package after the first processing sent to the real card manager, improve the charge packet transmission security, so that the real card manager will be real The prepaid package is sent to the real card for processing. In addition, the real card manager-side real card information list includes real card information of a real card connected to the real card manager, which may include information such as card number,
30 card authentication information, etc., whether or not the card authentication information is authenticated (Such as a bus card, a meal card, a shopping card, a membership card, a loyalty card,

etc.) issued by a bank card or a function card (such as a bus card, a meal card, a shopping card, a membership card, a loyalty card, etc.) issued by a bank for a regular channel (such as a bank, a bus company, etc.). In addition, the second secure transmission key of the smart cover can be referred to the description of the generation of the second secure transmission key of the smart cover, and will not be described in detail here. Optional, the real card manager can be set to save real card information for all or some of the real cards in the real card connected to it so that the user can make different settings based on the security requirements of the real card, for example, in real card management The settings on the device are not allowed to obtain real card information for some real cards, thus ensuring the security of these real cards.

The real card manager receives the data sent by the smart cover and sends the received data to the selected real card by using the real card manager side secure transmission key, and then the real card manager side secure transmission key For the smart cover with the real card manager to establish a secure connection generated when the selected real card: smart covers prompted the smart cover real card information list, and receive real card selection instructions to determine the real card, smart cover real card information The list is the list of real card managers that are retrieved from the real card manager. Specifically, the real card manager receives the data sent by the smart cover and then performs the second processing on the received data, which will be true and complete Data sent to the real card to ensure that the real card processing data authenticity and integrity, so as to ensure the safety of recharge. Among them, the real card manager-side secure transmission key can be generated by referring to the description of the real card manager side secure transmission key generation mode, and will not be described in detail here. The selection of the selected real card can be referred to the description of the selection of the actual card described above, and will not be described in detail here.

The selected real card receives the data sent by the real card manager and processes the received data to obtain the prepaid processing package. Specifically, the selected real card receives the real and complete data sent by the real card manager, the received data is processed in order to confirm that the transaction can be completed. The process of selecting the real card for transaction processing can refer to the process of dealing with the existing smart card.

The selected real card sends the prepaid processing packet to the real card manager;

The real card manager uses the real card manager to securely transmit the key to the prepaid processing packet and sends it to the card case.

The card receives the data sent by the real card manager and sends the received data to the payment platform after using the second secure transmission key of the smart cover to the payment platform. Specifically, the smart cover receives the selected real card processing of the data and send it to the payment platform in order to pay the platform for payment.

5 The account platform receives the payment success information transmitted from the payment platform and executes the recharge operation, wherein the payment success information is generated after the second processed data transmitted by the payment platform receiving packet and the transaction processing operation is performed. Specifically, after the payment is completed, the payment platform generates the payment success information and sends the payment success
10 information to the account platform so that the account platform knows that the payment is completed, thereby completing the recharge operation. Of course, the payment success information can also contain authentication information, so that the account platform to verify the success of the payment information, only after verification to complete the recharge, improve security.

Based on the above-mentioned way, the data interaction architecture of the invention can
15 complete the recharge of the account platform and extend the application of the data interaction architecture of the invention for the convenience of the user.

2. Recharging the real card

In an application scenario provided by the present embodiment, the user can realize the charging of the real card based on the above-described data interaction architecture, for example,
20 charging the bus card.

The following is a brief description of the implementation of this application scenario, but the invention is not limited thereto:

Smart cover from the real card manager connected to the real card, to determine the selected real card;

25 The charging platform obtains the card information of the selected real card through the simulation card, the smart cover and the real card manager, wherein the card information includes: the card number of the selected real card, the card authentication information;

The prepaid platform determines that the payment is successful and generates the prepaid package and sends it to the selected real card via the simulation card, the smart cover and the real
30 card manager. The prepaid package is prompted and confirmed by the smart cover.

The selected real card receives the data sent by the real card manager and performs the

recharge operation.

Based on the above brief description, the following provides a specific implementation, but the present invention is not limited thereto:

5 The card manager logs in to the real card manager, where the real card manager is connected to at least one real card and stores the real card manager side real card information list, the real card manager real card information list includes a real card manager The actual card information of the connected real card; in particular, the above-described card registration step can refer to the above description of the smart cover registration, and will not be described in detail here. Optional, the real card manager can be set to save the real card information of all or part of the real card in 10 the real card connected to it, forming a real card manager-side real card information list so that the user can, based on the security requirements for the real card Make different settings, for example, can be set in the real card manager does not allow access to some real card real card information, so as to ensure the security of these real cards.

15 The smart cover obtains the real card information list of the card manager, wherein the real card information list is the real card manager side real card information list obtained from the real card manager; in particular, the smart cover obtains the real card information list The relevant description of the list of real card information can be obtained by referring to the above-mentioned smart cover, which will not be described in detail here.

Smart covers of smart cover end of the real card information list;

20 The smart covers the real card selection command to determine the selected real card; in particular, the smart covers the selected real card to be prepaid card, such as the bus card, etc. At this point, the data card in the interaction interface can be used as a recharge card (Such as bus cards).

25 The card information receiving request includes at least the selected card number and the card authentication information of the real card; in particular, the user connects the simulation card with the charging platform through the contact type or the non-contact mode, and the card information receiving request, The rechargeable platform may include a front-end charging machine and a back-end charging processing platform such as a bus card charging platform, etc. The simulation card receives the card information acquisition request sent by the charging platform so as to obtain 30 the real card information of the selected real card.

The simulation card is sent to the card case after the first processing of the card information

acquisition request using the simulation card-side secure transmission key, wherein the simulation card-side secure transmission key is generated when the smart cover establishes a secure connection with the simulation card; After receiving the card information acquisition request, the simulation card sends the card information acquisition request to the smart cover by using the secure transmission key between the card and the card to improve the data transmission security. The generation process of the simulation card-side secure transmission key can be described in detail with reference to the description of the above-mentioned simulation card-side secure transmission key generation process.

The smart covers the data sent by the simulation card, and then uses the first security transmission key of the card to perform the second processing on the received data, and then uses the second security transmission key of the card to carry out the second processed data. Which is sent to the real card manager after processing, wherein the first secure transmission key of the smart cover is generated when the smart cover establishes a secure connection with the simulation card, and the second secure transmission key is the smart cover and the real card management In particular, the smart covers the second processing of the data sent by the simulation card and sends the data to the real card manager after the first processing, providing data transmission security and enabling the real card manager Get the card information acquisition request. The second secure transmission key and the second secure transmission key can be referred to the first secure transmission key and the second secure transmission key generation process of the smart cover, And then elaborate.

The real card manager receives the data sent by the smart cover, and sends the received data to the selected real card by using the real card manager side secure transmission key. The real card manager security transmission key is The card manager and the real card manager to establish a secure connection generated; in particular, the real card manager to send the data sent to the second package sent to the selected real card, so that the selected real card access card information acquisition request, Thereby returning the card information. The process of generating the secure transfer key of the real card manager side can refer to the description of the generation process of the secure transmission key of the real card manager side, and will not be described in detail here.

The selected real card will send the selected card information of the real card to the real card manager;

The real card manager uses the real card manager side secure transmission key to send the

card processing to the received card card information of the real card to the card sleeve;

5 The card receives the data sent by the real card manager, performs the second processing on the received data with the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to carry on the second processed data After the first processing sent to the simulation card;

The data sent by the simulation card receiving smart covers the second data of the received data by the simulation card side secure transmission key and sends it to the charging platform. Specifically, the simulation card sends the obtained card information to the charging platform to ensure that Fill the platform to know which real card to recharge.

10 After the payment platform is determined to be successful, the prepaid package will be generated and the prepaid package will be sent to the simulation card. Specifically, the prepaid platform can determine the payment success by collecting cash, collecting check, POS card completion, transfer and so on. The prepaid platform determines that the payment is successful and generates a prepaid package so that the selected real card is recharged according to the prepaid
15 package. Which includes at least: recharge the amount of recharge.

The simulation card receives the recharge box sent by the recharge platform, and uses the analog port security transmission key to carry out the first processing of the recharge pack to the smart cover;

20 The smart covers the data sent by the simulation card and prompts the second processed data after the second processing of the received data by using the first secure transmission key of the clip end;

The smart covers a confirmation instruction for indicating the correct data after the second processing, and sends the second processed data to the real card manager by first processing the second processed data with the second secure transmission key of the smart cover,

25 The real card manager receives the data sent by the smart cover, using the real card manager side secure transmission key to receive the data after the second processing sent to the selected real card;

The selected real card receives the second processed data sent by the real card manager and performs the recharge operation. Specifically, the selected real card is acquired to the prepaid
30 package, and the prepaid operation is performed according to the prepaid package, thereby completing the recharge.

Based on the above brief description, the present invention also provides a specific implementation by credit card charging, but the present invention is not limited thereto:

The card manager logs in to the real card manager, where the real card manager is connected to at least one real card and stores the real card manager side real card information list, the real card manager real card information list includes a real card manager The actual card information of the connected real card; in particular, the above-described card registration step can refer to the above description of the smart cover registration, and will not be described in detail here. Optional, the real card manager can be set to save the real card information of all or part of the real card in the real card connected to it, forming a real card manager-side real card information list so that the user can, based on the security requirements for the real card Make different settings, for example, can be set in the real card manager does not allow access to some real card real card information, so as to ensure the security of these real cards.

The smart cover obtains the real card information list of the card manager, wherein the real card information list is the real card manager side real card information list obtained from the real card manager; in particular, the smart cover obtains the real card information list The relevant description of the list of real card information can be obtained by referring to the above-mentioned smart cover, which will not be described in detail here.

Smart covers of smart cover end of the real card information list;

The smart covers the first real card selection instruction to determine the selected first real card; in particular, the smart cover determines that the selected first real card is a debit card, such as a bank card, etc., at this time, the simulation in the data interaction architecture Cards can be used as debit cards (such as bank cards).

The first card information acquisition request includes at least the selected card number and the card authentication information of the first real card; in particular, the user passes the simulation card or the contact card in a contactless or non-contact manner, and the first card information acquisition request includes the first card information acquisition request, (Such as a POS machine, etc.) and a payment processing platform (e.g., a bank background), which connects the simulation card with the debit terminal for charging, the simulation card receiving payment platform is transmitted, and the payment desk is connected to the payment terminal The first card information acquisition request in order to obtain the real card information of the selected first real card.

The simulation card sends the first card information acquisition request to the card case by using the simulation card side secure transmission key, and the simulation card side secure transmission key is generated when the smart cover establishes a secure connection with the simulation card; And the simulation card receives the first card information acquisition request and sends the first card information acquisition request to the smart cover after the first card information acquisition request with the secure transmission key between the card and the card to improve the data transmission security. The generation process of the simulation card-side secure transmission key can be described in detail with reference to the description of the above-mentioned simulation card-side secure transmission key generation process.

The smart covers the data sent by the simulation card, and then uses the first security transmission key of the card to perform the second processing on the received data, and then uses the second security transmission key of the card to carry out the second processed data. Which is sent to the real card manager after processing, wherein the first secure transmission key of the smart cover is generated when the smart cover establishes a secure connection with the simulation card, and the second secure transmission key is the smart cover and the real card management In particular, the smart covers the second processing of the data sent by the simulation card and sends the data to the real card manager after the first processing, providing data transmission security and enabling the real card manager The first card information acquisition request is obtained. The second secure transmission key and the second secure transmission key can be referred to the first secure transmission key and the second secure transmission key generation process of the smart cover, And then elaborate.

The real card manager receives the data sent by the smart cover and sends the selected data to the selected first real card by using the real card manager side secure transmission key, and then the real card manager side secure transmission secret The key card manager generates a secure connection with the real card manager; in particular, the real card manager sends a second processing of the data sent by the smart cover to the selected first real card so that the selected first real card Obtains the first card information acquisition request, thereby returning the card information. The process of generating the secure transfer key of the real card manager side can refer to the description of the generation process of the secure transmission key of the real card manager side, and will not be described in detail here.

The selected first real card sends the selected card information of the first real card to the real

card manager;

The real card manager uses the real card manager side secure transmission key to carry out the first processing to the received card information of the first real card and sends it to the smart cover;

5 The card receives the data sent by the real card manager, performs the second processing on the received data with the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to carry on the second processed data After the first processing sent to the simulation card;

10 The data sent from the simulation card receiving card is sent to the payment platform by the second processing of the received data using the simulation card side secure transmission key; in particular, the simulation card sends the card information of the first real card acquired to Payment platform to ensure that the payment platform to know which real card to use the charge.

15 The simulation card receives the chargeback request sent by the payment platform and sends the charge request to the smart cover first by using the simulation card side secure transmission key; in particular, the chargeback request may include at least the charge amount.

The smart covers the data sent by the simulation card, the second processed data is processed by the first secure transmission key of the smart cover, and the second processed data is prompted; in particular, the smart cover can request the charge Display or voice playback so that the user can confirm the information in the chargeback request.

20 The smart covers a confirmation command for indicating the correct data of the second processed data, and sends the second processed data to the real card manager by using the card second end secure transmission key; The user confirms the correct confirmation on the smart cover (for example, presses the confirmation key, selects the confirmation option in the menu, etc.) to generate a confirmation instruction for confirming the receipt of the charge, and the smart covers
25 the confirmation instruction so that the smart cover continues The follow-up operation; of course, if the user to confirm the charge request is a problem, you can cancel the operation on the card in order to cancel the transaction. The acknowledgment command received by the smart cover for indicating the correct data of the second processed data may be generated for the confirmation physical button provided separately on the ferrule or may be generated by a confirmation virtual
30 key on the touch screen of the smart cover, or (Such as a microphone) received by the confirmation function generated in the menu displayed on the smart cover screen, or a voice

confirmation device received by the voice collection device (for example, Mike) of the smart cover and verified by the fingerprint collection device. It is possible to receive the iris confirmation instruction and verify the pass generated after receiving the fingerprint confirmation instruction and verifying the pass generated, or the iris acquisition device which can be used for the smart cover, and may, for example, be generated in any other way, and not in the present invention limit.

The real card manager receives the data sent by the smart covers, uses the real card manager side secure transmission key to carry on the second processing to the received data to the selected first real card;

The selected first real card receives the data sent by the real card manager and processes the received data to process the data obtained after the transaction processing to the real card manager; in particular, the selected first real card receives Real card manager to send the real and complete data, the received data transaction processing in order to confirm the transaction can be completed, the selected first real card transaction processing process can refer to the existing smart card transaction processing process, No longer elaborate here.

The real card manager receives the data sent by the selected first real card and sends the data to the smart cover first by processing the received data with the real card manager secure transmission key;

The card receives the data sent by the real card manager and performs the second processing on the received data using the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to correct the second processed. The data is sent to the simulation card after the first processing;

Simulating the data sent by the card receiving card and sending the second data to the payment platform for the charging operation by using the simulation card end secure transmission key; in particular, the payment platform receives the selected value of the simulation card transmission. The first real card transaction processing data, and verify the implementation of the charge after the implementation of the operation, of course, in the payment platform after the completion of the charge operation, you can also generate payment success information in order to prompt the user to pay success.

In addition, the user can select the prepaid card (for example, the bank card) in order to recharge the card to be prepaid after the payment is confirmed.

The smart covers the second real card selection instruction to determine the selected second

real card; in particular, the smart cover determines that the selected second real card is the card to be recharged, such as a bus card, etc. At this point, the simulation in the data interaction architecture Cards can be used as cards (such as bus cards) to be recharged.

The second card information acquisition request includes at least the card number and the card authentication information of the selected second real card; in particular, the user enters the simulation card by contact or non-contact mode, and the second card information acquisition request, And the charging platform may include a front-end charging machine and a back-end charging processing platform such as a bus card charging platform, etc. The simulation card receives the second card information acquisition request sent by the charging platform so as to obtain the selected second real card The real card information.

The simulation card is sent to the smart cover after the first processing of the second card information acquisition request by using the simulation card-side secure transmission key, wherein the simulation card-side secure transmission key is generated when the card is set up securely with the simulation card; , The simulation card receives the second card information acquisition request and sends the card information acquisition request to the card case after the first card processing using the secure transmission key between the card and the card to improve the data transmission security. The generation process of the simulation card-side secure transmission key can be described in detail with reference to the description of the above-mentioned simulation card-side secure transmission key generation process.

The smart covers the data sent by the simulation card, and then uses the first security transmission key of the card to perform the second processing on the received data, and then uses the second security transmission key of the card to carry out the second processed data. Which is sent to the real card manager after processing, wherein the first secure transmission key of the smart cover is generated when the smart cover establishes a secure connection with the simulation card, and the second secure transmission key is the smart cover and the real card management In particular, the smart covers the second processing of the data sent by the simulation card and sends the data to the real card manager after the first processing, providing data transmission security and enabling the real card manager Get the card information acquisition request. The second secure transmission key and the second secure transmission key can be referred to the first secure transmission key and the second secure transmission key generation process of the smart cover, And then elaborate.

The real card manager receives the data sent by the smart cover, and sends the received data to the selected second real card by using the real card manager side secure transmission key, and then the real card manager side secure transmission density The key card manager generates a secure connection to the real card manager; in particular, the real card manager sends the data sent by the smart cover to the selected real card for the selected second real card to obtain the card Information acquisition request, which will return the card information. The process of generating the secure transfer key of the real card manager side can refer to the description of the generation process of the secure transmission key of the real card manager side, and will not be described in detail here.

The selected second real card will send the selected card information of the real card to the real card manager;

The real card manager sends the card information of the selected second real card to the smart cover by using the real card manager side secure transmission key to perform the first processing;

The card receives the data sent by the real card manager, performs the second processing on the received data with the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to carry on the second processed data After the first processing sent to the simulation card;

The data sent from the simulation card receiving card is sent to the charging platform by the second processing of the received data using the simulation card side secure transmission key; in particular, the simulation card sends the card information of the second real card acquired to Recharge the platform, so as to ensure that the recharge platform for which real card to recharge.

The emulation card receives the recharge pack generated by the charging platform; in particular, the charging platform determines that the payment is successful and obtains the card information of the selected second real card, generates the prepaid package so that the selected second real card can carry out the refill operation according to the prepaid package The Which includes at least: recharge the amount of recharge.

The simulation card is sent to the card case by first processing the prepaid packet using the simulation card end secure transmission key;

The smart covers the data sent by the simulation card and prompts the second processed data after the second processing of the received data by using the first secure transmission key of the clip end;

The smart cover covers a confirmation instruction for indicating the correct data after the second processing, and sends the second processed data to the real card manager by first processing the second processed data with the second secure transmission key of the smart cover,

The real card manager receives the data sent by the smart cover, uses the real card manager side secure transmission key to carry on the second processing to the received data to the selected second real card;

The selected second real card receives the second processed data sent by the real card manager and performs the recharging operation. Specifically, the selected second real card is fetched to the prepaid package, and the refill operation is performed according to the refill pack, thereby completing the refill.

Based on the above-mentioned way, the data interaction architecture of the present invention can complete the recharge of the real card and extend the application of the data interworking architecture of the invention for the convenience of the user.

3. The second real card recharging the first real card

In an application scenario provided by the present embodiment, based on the data interaction architecture described above, the user can realize the recharge of the real card by the real card, for example, by charging the bus card to the bus card or by charging the card with the bank card. In this application scenario, the second real card is different from the first real card type, the second real card is a real card that can be debited, and the first real card is a real card to be charged.

The following is a brief description of the implementation of this application scenario, but the invention is not limited thereto:

Smart cover from the real card manager connected to the real card, determine the selected first real card;

The charging platform obtains the card information of the selected first real card through the simulation card, the smart cover and the real card manager, wherein the card information includes the selected first real card card number and the card authentication information,

Smart cover from the real card manager connected to the real card, determine the selected second real card;

Payment platform through the smart covers, the real card manager and the selected second real card charge processing;

Smart cover from the real card manager connected to the real card, determine the selected

first real card;

The prepaid platform generates the prepaid package and sends it to the selected real card through the simulation card, the smart cover and the real card manager, where the prepaid package is prompted and confirmed by the smart cover;

5 The selected real card receives the data sent by the real card manager and performs the recharge operation.

Based on the above brief description, the following provides a specific implementation, but the present invention is not limited thereto:

10 The card manager logs in to the real card manager, where the real card manager is connected to at least one real card and stores the real card manager side real card information list, the real card manager real card information list includes a real card manager The actual card information of the connected real card; in particular, the above-described card registration step can refer to the above description of the smart cover registration, and will not be described in detail here. Optional, the real card manager can be set to save the real card information of all or part of the real card in
15 the real card connected to it, forming a real card manager-side real card information list so that the user can, based on the security requirements for the real card Make different settings, for example, can be set in the real card manager does not allow access to some real card real card information, so as to ensure the security of these real cards.

20 The smart cover obtains the real card information list of the card manager, wherein the real card information list is the real card manager side real card information list obtained from the real card manager; in particular, the smart cover obtains the real card information list The relevant description of the list of real card information can be obtained by referring to the above-mentioned smart cover, which will not be described in detail here.

Smart covers of smart cover end of the real card information list;

25 The smart covers the first real card selection instruction to determine the selected first real card; in particular, the smart cover determines that the selected first real card is a card to be prepaid, such as a bus card, etc. At this point, the simulation in the data interaction architecture Cards can be used as cards (such as bus cards) to be recharged.

30 The first card information acquisition request includes at least the selected first real card card number and the card authentication information; in particular, the user enters the simulation card by contact or non-contact mode, and the first card information acquisition request, And the

recharge platform can be connected, the recharge platform can include front-end recharge machine and background recharge processing platform, such as: bus card recharge platform or electric card recharge platform, the simulation card and the front-end recharge machine connected to simulate the card to receive the recharge platform to send The first card information acquisition request is made in order to obtain the real card information of the selected first real card.

The simulation card sends the first card information acquisition request to the card case by using the simulation card side secure transmission key, and the simulation card side secure transmission key is generated when the smart cover establishes a secure connection with the simulation card; And the simulation card receives the first card information acquisition request and sends the first card information acquisition request to the smart cover after the first card information acquisition request with the secure transmission key between the card and the card to improve the data transmission security. The generation process of the simulation card-side secure transmission key can be described in detail with reference to the description of the above-mentioned simulation card-side secure transmission key generation process.

The smart covers the data sent by the simulation card, and then uses the first security transmission key of the card to perform the second processing on the received data, and then uses the second security transmission key of the card to carry out the second processed data. Which is sent to the real card manager after processing, wherein the first secure transmission key of the smart cover is generated when the smart cover establishes a secure connection with the simulation card, and the second secure transmission key is the smart cover and the real card management In particular, the smart covers the second processing of the data sent by the simulation card and sends the data to the real card manager after the first processing, providing data transmission security and enabling the real card manager The first card information acquisition request is obtained. The second secure transmission key and the second secure transmission key can be referred to the first secure transmission key and the second secure transmission key generation process of the smart cover, And then elaborate.

The real card manager receives the data sent by the smart cover and sends the selected data to the selected first real card by using the real card manager side secure transmission key, and then the real card manager side secure transmission secret The key card manager generates a secure connection with the real card manager; in particular, the real card manager sends a second processing of the data sent by the smart cover to the selected first real card so that the selected first

real card Obtains the first card information acquisition request, thereby returning the card information. The process of generating the secure transfer key of the real card manager side can refer to the description of the generation process of the secure transmission key of the real card manager side, and will not be described in detail here.

5 The selected first real card sends the selected card information of the first real card to the real card manager;

 The real card manager uses the real card manager side secure transmission key to carry out the first processing to the received card information of the first real card and sends it to the smart cover;

10 The card receives the data sent by the real card manager, performs the second processing on the received data with the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to carry on the second processed data After the first processing sent to the simulation card;

 The data sent from the simulation card receiving card is sent to the charging platform by the
15 second processing of the received data using the simulation card side secure transmission key; in particular, the simulation card sends the card information of the first real card to the Recharge the platform, so as to ensure that the recharge platform for which real card to recharge.

 The smart covers the recharge card of the prepaid platform, and displays the real card information list of the smart cover; in particular, the smart covers the recharge label sent by the
20 charging platform to indicate which card is charged and prompts the user to select the first real card To charge card) recharge the second real card (charge card). The recharge symbol may contain a first real card card number, order number, recharge amount, etc., or a combination thereof, to be charged.

 The smart covers the second real card selection command to determine the selected second
25 real card; in particular, the smart cover determines that the selected second real card is a debit card, such as a bank card.

 The second card information acquisition request includes at least the card number of the selected second real card and the card authentication information; in particular, the user enters the simulation card by contact or non-contact mode, and the second card information acquisition
30 request, (Such as a POS machine, etc.) and a payment processing platform (e.g., a bank background), which connects the simulation card with the debit terminal for charging, the

simulation card receiving payment platform is transmitted, and the payment desk is connected to the payment terminal. The second card information acquisition request is sent in order to obtain the real card information of the selected second real card.

5 The simulation card is sent to the smart cover after the first processing of the second card information acquisition request by using the simulation card-side secure transmission key, wherein the simulation card-side secure transmission key is generated when the card is set up securely with the simulation card; , The simulation card receives the second card information acquisition request and sends the second card information acquisition request to the smart cover after the second card information acquisition request with the secure transmission key between the card and the card to
10 improve the data transmission security. The generation process of the simulation card-side secure transmission key can be described in detail with reference to the description of the above-mentioned simulation card-side secure transmission key generation process.

The smart cover covers the data sent by the simulation card, and then uses the first security transmission key of the card to perform the second processing on the received data, and then uses
15 the second security transmission key of the card to carry out the second processed data. Which is sent to the real card manager after processing, wherein the first secure transmission key of the smart cover is generated when the smart cover establishes a secure connection with the simulation card, and the second secure transmission key is the smart cover and the real card management. In particular, the smart cover covers the second processing of the data sent by the simulation card and sends
20 the data to the real card manager after the first processing, providing data transmission security and enabling the real card manager to obtain a second card information acquisition request. The second secure transmission key and the second secure transmission key can be referred to the first secure transmission key and the second secure transmission key generation process of the smart cover, And then elaborate.

25 The real card manager receives the data sent by the smart cover, and sends the received data to the selected second real card by using the real card manager side secure transmission key, and then the real card manager side secure transmission density. The key card manager generates a secure connection with the real card manager; in particular, the real card manager sends a second processing of the data sent by the smart cover to the selected second real card so that the selected
30 second real card obtains the second card information acquisition request, thereby returning the card information. The process of generating the secure transfer key of the real card manager side

can refer to the description of the generation process of the secure transmission key of the real card manager side, and will not be described in detail here.

The selected second real card sends the selected card information of the second real card to the real card manager;

5 The real card manager sends the card information of the selected second real card to the smart cover by using the real card manager side secure transmission key to perform the first processing;

10 The card receives the data sent by the real card manager, performs the second processing on the received data with the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to carry on the second processed data After the first processing sent to the simulation card;

The data sent from the simulation card receiving card is sent to the payment platform by the second processing of the received data using the simulation card side secure transmission key; in particular, the simulation card sends the card information of the second real card acquired to Payment platform to ensure that the payment platform to know which real card to use the charge.

15 The simulation card receives a chargeback request sent by the payment platform and sends the charge request to the smart cover first by using the simulation card-side secure transmission key; in particular, the chargeback request may include at least the amount of the charge and the first real card card number.

20 The smart covers the data sent by the simulation card, the second processed data is processed by the first secure transmission key of the smart cover, and the second processed data is prompted; in particular, the smart cover can request the charge Display or voice playback so that the user can confirm the information in the chargeback request.

25 The smart covers a confirmation command for indicating the correct data of the second processed data, and sends the second processed data to the real card manager by using the card second end secure transmission key; The user confirms the correct confirmation on the smart cover (for example, presses the confirmation key, selects the confirmation option in the menu, etc.) to generate a confirmation instruction for confirming the receipt of the charge, and the smart covers the confirmation instruction so that the smart cover continues The follow-up operation; of course, if the user to confirm the charge request is a problem, you can cancel the operation on the card in
30 order to cancel the transaction. The acknowledgment command received by the smart cover for indicating the correct data of the second processed data may be generated for the confirmation

physical button provided separately on the ferrule or may be generated by a confirmation virtual key on the touch screen of the smart cover, or (Such as a microphone) received by the confirmation function generated in the menu displayed on the smart cover screen, or a voice confirmation device received by the voice collection device (for example, Mike) of the smart cover and verified by the fingerprint collection device It is possible to receive the iris confirmation instruction and verify the pass generated after receiving the fingerprint confirmation instruction and verifying the pass generated, or the iris acquisition device which can be used for the smart cover, and may, for example, be generated in any other way, and not in the present invention limit.

The real card manager receives the data sent by the smart cover, uses the real card manager side secure transmission key to carry on the second processing to the received data to the selected second real card;

The selected second real card receives the data sent by the real card manager and processes the received data to process the data obtained after the transaction processing to the real card manager. Specifically, the selected second real card receives Real card manager to send the real and complete data, the received data transaction processing in order to confirm the transaction can be completed, the selected second real card transaction processing process can refer to the existing smart card transaction processing process , No longer elaborate here.

The real card manager receives the selected data from the selected second real card and sends the data to the smart cover first by processing the received data with the real card manager secure transmission key;

The card receives the data sent by the real card manager and performs the second processing on the received data using the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to correct the second processed The data is sent to the simulation card after the first processing;

Simulating the data sent by the card receiving the card and sending the data to the payment platform after the second processing of the received data using the simulation card side secure transmission key;

The simulation card is first sent to the smart cover after the first payment of the payment success information by using the simulation card side secure transmission key, wherein the payment success information is generated after the payment payment is successfully performed by the payment platform; in particular, the payment platform, upon receiving the selected After the

verification of the data, after the verification is completed, the charge operation is executed, and after the completion of the charge operation, the payment success information is generated, and the payment success information may include the selected first real card card number or the other Card recharge information, as long as the recharge platform for the follow-up to know which card to
5 recharge the successful implementation of the charge can be.

The smart covers the data sent by the simulation card and carries on the second processing to the received data using the first secure transmission key of the clip end, prompting the smart cover's real card information list;

The smart covers the first real card selection command to determine the selected first real
10 card; in particular, the user again selects the first real card in order to complete the refill operation for the first real card.

The charging card receives the prepaid packet sent by the charging platform, wherein the prepaid package is generated by the prepaid platform to receive the payment success information; in particular, the payment platform can also send the payment success information directly to the
15 charging platform, or the smart cover will pay the success message To the up-to-date platform so that the up-to-date platform is aware of the payment success and generates a prepaid package to send the prepaid package to the selected first real card to complete the recharge.

The simulation card is sent to the card case by first processing the prepaid packet using the simulation card end secure transmission key;

20 The smart covers the data sent by the simulation card and prompts the second processed data after the second processing of the received data by using the first secure transmission key of the clip end;

The smart covers a confirmation instruction for indicating the correct data after the second processing, and sends the second processed data to the real card manager by first processing the
25 second processed data with the second secure transmission key of the smart cover,

The real card manager receives the data sent by the smart covers, uses the real card manager side secure transmission key to carry on the second processing to the received data to the selected first real card;

The first real card receives the data sent by the real card manager and performs the recharge
30 operation. Specifically, the selected first real card is fetched to the prepaid package, and the prepaid operation is performed according to the refill pack, thereby completing the refill.

Based on the above-described manner, the data interaction architecture of the present invention can complete the use of the second real card to recharge the first real card and extend the application of the data interaction architecture of the present invention for user convenience.

4. The account recharging the real card

5 In an application scenario provided by the present embodiment, the user can realize the recharge of the real card by the user based on the above-mentioned data interaction structure, for example, by paying the treasure or the online banking.

The following is a brief description of the implementation of this application scenario, but the invention is not limited thereto:

10 Smart cover from the real card manager connected to the real card, to determine the selected real card;

The charging platform obtains the card information of the selected real card through the simulation card, the smart cover and the real card manager, wherein the card information includes: the card number of the selected real card, the card authentication information;

15 Smart covers to pay the payment platform, payment platform to obtain the recharge mark after the charge processing;

The prepaid platform receives the payment success information generated by the payment platform and generates the prepaid package and sends it to the selected real card through the simulation card, the smart cover and the real card manager, wherein the prepaid package is
20 prompted and confirmed by the smart cover;

The selected real card receives the data sent by the real card manager and performs the recharge operation.

Based on the above brief description, the following provides a specific implementation, but the present invention is not limited thereto:

25 The card manager logs in to the real card manager, where the real card manager is connected to at least one real card and stores the real card manager side real card information list, the real card manager real card information list includes a real card manager The actual card information of the connected real card; in particular, the above-described card registration step can refer to the above description of the smart cover registration, and will not be described in detail here. Optional,
30 the real card manager can be set to save the real card information of all or part of the real card in the real card connected to it, forming a real card manager-side real card information list so that the

user can, based on the security requirements for the real card Make different settings, for example, can be set in the real card manager does not allow access to some real card real card information, so as to ensure the security of these real cards.

The smart cover obtains the real card information list of the card manager, wherein the real card information list is the real card manager side real card information list obtained from the real card manager; in particular, the smart cover obtains the real card information list The relevant description of the list of real card information can be obtained by referring to the above-mentioned smart cover, which will not be described in detail here.

Smart covers of smart cover end of the real card information list;

The smart covers the real card selection command to determine the selected real card; in particular, the smart covers the selected real card to be prepaid card, such as the bus card, etc. At this point, the data card in the interaction interface can be used as a recharge card (Such as bus cards).

The card information receiving request includes at least the selected card number and the card authentication information of the real card; in particular, the user connects the simulation card with the charging platform through the contact type or the non-contact mode, and the card information receiving request, The rechargeable platform may include a front-end charging machine and a back-end charging processing platform such as a bus card charging platform, etc. The simulation card receives the card information acquisition request sent by the charging platform so as to obtain the real card information of the selected real card.

The simulation card is sent to the card case after the first processing of the card information acquisition request using the simulation card-side secure transmission key, wherein the simulation card-side secure transmission key is generated when the smart cover establishes a secure connection with the simulation card; After receiving the card information acquisition request, the simulation card sends the card information acquisition request to the smart cover by using the secure transmission key between the card and the card to improve the data transmission security. The generation process of the simulation card-side secure transmission key can be described in detail with reference to the description of the above-mentioned simulation card-side secure transmission key generation process.

The smart covers the data sent by the simulation card, and then uses the first security transmission key of the card to perform the second processing on the received data, and then uses

the second security transmission key of the card to carry out the second processed data. Which is sent to the real card manager after processing, wherein the first secure transmission key of the smart cover is generated when the smart cover establishes a secure connection with the simulation card, and the second secure transmission key is the smart cover and the real card management In particular, the smart covers the second processing of the data sent by the simulation card and sends the data to the real card manager after the first processing, providing data transmission security and enabling the real card manager Get the card information acquisition request. The second secure transmission key and the second secure transmission key can be referred to the first secure transmission key and the second secure transmission key generation process of the smart cover, And then elaborate.

The real card manager receives the data sent by the smart cover, and sends the received data to the selected real card by using the real card manager side secure transmission key. The real card manager security transmission key is The card manager and the real card manager to establish a secure connection generated; in particular, the real card manager to send the data sent to the second package sent to the selected real card, so that the selected real card access card information acquisition request, Thereby returning the card information. The process of generating the secure transfer key of the real card manager side can refer to the description of the generation process of the secure transmission key of the real card manager side, and will not be described in detail here.

The selected real card will send the selected card information of the real card to the real card manager;

The real card manager uses the real card manager side secure transmission key to send the card processing to the received card card information of the real card to the card sleeve;

The card receives the data sent by the real card manager, performs the second processing on the received data with the second secure transmission key of the smart cover, and then uses the first secure transmission key of the smart cover to carry on the second processed data After the first processing sent to the simulation card;

The data sent by the simulation card receiving smart covers the second data of the received data by the simulation card side secure transmission key and sends it to the charging platform. Specifically, the simulation card sends the obtained card information to the charging platform to ensure that Fill the platform to know which real card to recharge.

In particular, the card can log on to the payment platform, the payment platform can be Alipay,

or online banking, in order to complete the charge operation, such as the user login Alipay directly from the Alipay debit, or user login online banking directly from the online banking buckle Section, or user login Alipay and bundled with Alipay online banking charge.

5 The payment success information transmitted by the payment platform is generated by the payment platform after the payment operation is performed; in particular, the payment platform generates the payment success information after the payment is completed and transmits the payment success information to the smart cover so that the user knows the payment is successful. The payment platform can also obtain the recharge ID before the payment operation is carried out, and the recharge record can be obtained by the following method: The first embodiment of the
10 simulation card receives the recharge record sent by the charging platform and performs the first processing on the recharge ID using the simulation card security transmission key And then sent to the smart covers, the smart covers the data sent by the simulation card, using the first secure transmission key of the card to the received data for the second processing to be recharged and sent by the card to the payment platform. Wherein the prepaid identification is generated after the
15 charge station receives the data after the second processing of the simulation card, and in particular, the prepaid platform obtains the card information of the first real card sent by the simulation card, and generates a recharge flag to indicate which Real card to recharge and recharge the amount of the recharge mark can be generated for the recharge of the order number and so on. Second, the recharge platform in the simulation card after receiving the second processed data generated after
20 the recharge ID, directly to the recharge ID sent to the payment platform. In addition, the payment platform pays in accordance with the recharging identity so as to know which real card is to be paid and the amount paid.

The charging card receives the prepaid packet sent by the charging platform, wherein the prepaid package is generated by the payment platform after receiving the payment success
25 information generated by the payment platform; in particular, the payment platform also sends the payment success information to the charging platform, or the payment platform will pay successfully The information is sent to the smart cover and sent by the smart cover to the recharge platform so that the prepaid platform knows the payment is successful and generates a prepaid package to send the prepaid package to the selected real card to complete the recharge.

30 The simulation card is sent to the card case by first processing the prepaid packet using the simulation card end secure transmission key;

The smart covers the data sent by the simulation card and prompts the second processed data after the second processing of the received data by using the first secure transmission key of the clip end;

5 The smart covers a confirmation instruction for indicating the correct data after the second processing, and sends the second processed data to the real card manager by first processing the second processed data with the second secure transmission key of the smart cover,

The real card manager receives the data sent by the smart cover, using the real card manager side secure transmission key to receive the data after the second processing sent to the selected real card;

10 The real card receives the data sent by the real card manager and performs the recharge operation. Specifically, the selected real card is acquired to the prepaid package, and the prepaid operation is performed according to the prepaid package, thereby completing the recharge.

Based on the above-mentioned way, the data interaction architecture of the invention can complete the recharge of the real card by using the account, and expand the application of the data
15 interaction architecture of the invention, and is convenient for the user to use.

In embodiments of the present disclosure, for all the normal data interaction 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
20 message to a user terminal (such as a smart phone, a tablet computer, etc.), so as to prompt the user of abnormal position of 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
25 preferred embodiment of the present disclosure includes other 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.

30 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 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.

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.

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 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 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;

15 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.

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:

25 establishing a secure 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.

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;

25 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 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;

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. 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 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.