

Data Storage System and Method Used For the Security Information Interaction

Field of the Invention

5 The present invention relates to a data storage system and method, and more particularly, to a data storage system and method used for the security information interaction.

Background

10 Nowadays, with the increasingly development of network technology and increasingly enrichment of business types of different fields (e.g. the internet-based financial transaction field), there is an increasingly growing demand for the data storage system and method used for the security information interaction, therefore, the security data storage system and method become more and more important.

15 Typically, the existing security data storage systems (for example, in the applications which adopt the authentication technology such as a digital certificate based on public key cryptography system, a dynamic password or the like, a USBKey is usually used to store the digital certificate and associated key pair) include the following two implementation approach: (1)
20 both a user password and an unlock password are used in the security data storage system (including a security data storage device), said user password is used for authenticating the identity of the user of the security data storage device, and said unlock password is used for unlocking the security data storage device (when the number of times that the error user passwords are
25 entered continuously reach a predetermined number of times, said security data storage device is locked automatically), so as to cause said user password to recovery to an initial state, wherein, the user password of said security data storage device is initialized by the manufacturer and can be reset by the user,

whereas the unlock passwords are all the same (for example, the USBKeys belonging to the same batch have the same unlock passwords); (2) the initialization and reset of the user password are not supported (for example, the PIN code is not supported) in the security data storage system, i.e., once
5 the security data storage device is locked, the user must use a new security data storage device (e.g. the USBKey) and re-download new security information data (such as the digital certificate).

However, the first implementation approach described above has the following problems: due to the unlock passwords are all the same, once the
10 unlock password has been divulged, then any security data storage device can be unlocked, thus there exist largely potential security risks.

The second implementation approach described above has the following problems: the use cost of the user increases (for example, once the security data storage device is locked, a new security data storage device needs to be
15 used), and the complexity of use is significantly increased (for example, to re-download new security information data).

Therefore, there exists the needs for providing a data storage system and method used for the security information interaction, which have the high degree of security and are convenient and easy to use.

20

Summary of the invention

In order to solve the problems presented in the existing technical solutions described above, the present invention proposes a data storage system and method used for the security information interaction.

25 The object of the present invention is realized through the following technical solutions:

A data storage system used for the security information interaction, said data storage system used for the security information interaction comprising:

a security information storage device for storing and providing the data information related to the security information interaction;

an unlock password generating device for generating the unlock password corresponding to said security information storage device based on original parameters extracted from said security information storage device, and writing the
5 unlock password into said security information storage device; and

an unlock server for generating the unlock password corresponding to said security information storage device based on original parameters acquired from said security information storage device when said security information storage
10 device is locked, and using said unlock password to unlock said locked security information storage device.

In the solutions disclosed above, preferably, said original parameters are at least one factor being capable of uniquely identifying said security information storage device.

15 In the solutions disclosed above, preferably, said original parameters are the identifier of said security information storage device.

In the solutions disclosed above, preferably, said data information related to the security information interaction include an unlock password, a user password and business authentication data.

20 In the solutions disclosed above, preferably, said security information storage device further comprises:

a data communication interface for completing the data communication with external devices;

an unlock password initialization module for providing original parameters
25 corresponding to said security information storage device in response to an original parameters extracting request message from said unlock password generating device, and storing the unlock password generated by the unlock password generating device into a data storage module;

an unlock module for providing original parameters corresponding to said

security information storage device according to the original parameters extracting request message from said unlock server, and unlocking said security information storage device based on the unlock password in an unlock request message from said unlock server;

5 a locking module for locking said security information storage device when a predetermined condition is satisfied; and

 a data storage module for storing said data information related to the security information interaction.

 In the solutions disclosed above, preferably, said security information storage
10 device further comprises an information reset module. Said information reset module is used to initialize the predetermined items in said data information related to the security information interaction when said security information storage device is unlocked.

 In the solutions disclosed above, preferably, said data communication interface
15 is a USB interface.

 In the solutions disclosed above, preferably, said unlock password generating device further comprises:

 an original parameters extracting module for sending said original parameters extracting request message to said security information storage device, and
20 transmitting the original parameters acquired from said security information storage device to a password generating module; and

 a password generating module for generating an unlock password corresponding to said security information storage device based on said original parameters and by means of invoking a first dynamic link library, and transmitting
25 the generated unlock password to said security information storage device.

 In the solutions disclosed above, preferably, said first dynamic link library is set by a service provider or the relevant third party.

 In the solutions disclosed above, preferably, said unlock server further comprises:

an original parameters acquiring module for sending an original parameters extracting request message to said security information storage device, and transmitting the original parameters acquired from said security information storage device to an unlock password generating module;

5 an unlock password generating module for generating an unlock password corresponding to said security information storage device based on said original parameters and by means of invoking the second dynamic link library, and transmitting the generated unlock password to an unlock initiating module; and

an unlock initiating module for configuring an unlock request message based
10 on the generated unlock password, and transmitting said unlock request message to said security information storage device.

In the solutions disclosed above, preferably, said second dynamic link library is set by the manufacturer of said security information storage device.

In the solutions disclosed above, preferably, said security information storage
15 device is a USBKey.

The object of the present invention can also be realized through the following technical solutions:

A data storage method used for the security information interaction, said data storage method used for the security information interaction comprising the
20 following steps:

(A1) an unlock password generating device generating an unlock password corresponding to a security information storage device based on the original parameters extracted from said security information storage device, and writing the unlock password into said security information storage device;

25 (A2) an unlock server generating the unlock password corresponding to said security information storage device based on the original parameters acquired from said security information storage device when said security information storage device is locked, and using said unlock password to unlock said locked security information storage device;

(A3) said security information storage device communicating with a user terminal via a data communication interface when said security information storage device is in a non-locked state, so as to complete the interaction of the security information.

5 In the solutions disclosed above, preferably, said original parameters are at least one factor being capable of uniquely identifying said security information storage device.

 In the solutions disclosed above, preferably, said original parameters are the identifier of said security information storage device.

10 In the solutions disclosed above, preferably, said security information is business authentication data.

 In the solutions disclosed above, preferably, said data storage method used for the security information interaction further comprises:

15 (A4) locking said security information storage device when a predetermined condition is satisfied.

 In the solutions disclosed above, preferably, said step (A2) further comprises: initializing predetermined items when said security information storage device is unlocked.

20 In the solutions disclosed above, preferably, said data communication interface is a USB interface.

 In the solutions disclosed above, preferably, said step (A1) further comprises:

 (B1) sending an original parameters extracting request message to said security information storage device, so as to acquire the original parameters from said security information storage device; and

25 (B2) generating an unlock password corresponding to said security information storage device based on said original parameters and by means of invoking a first dynamic link library, and transmitting the generated unlock password to said security information storage device.

 In the solutions disclosed above, preferably, said first dynamic link library is

set by a service provider or the relevant third party.

In the solutions disclosed above, preferably, said step (A2) further comprises:

(C1) sending an original parameters extracting request message to said security information storage device, so as to acquire the original parameters from
5 said security information storage device;

(C2) generating an unlock password corresponding to said security information storage device based on said original parameters and by means of invoking the second dynamic link library; and

(C3) configuring an unlock request message based on the generated unlock
10 password, and transmitting said unlock request message to said security information storage device.

In the solutions disclosed above, preferably, said second dynamic link library is set by the manufacturer of said security information storage device.

In the solutions disclosed above, preferably, said security information storage
15 device is a USBKey.

The data storage system and method used for the security information interaction disclosed in the present invention have the following advantages: (1) since different security information storage devices have different unlock passwords, the potential security risks due to the divulgement of the unlock
20 passwords are reduced; (2) the complexity of the unlock process is reduced, and the maintain cost of the user for the security information storage device is reduced at the same time; (3) since said first dynamic link library and said second dynamic link library are set by different providers, the details (e.g., which key algorithm is adopted) of generating and writing the unlock
25 password are not visible to the external, thereby further reducing the potential security risks existed in the generating and writing process of the unlock password on the whole.

Brief description of the drawings

The technical features and advantages of the present invention will be better appreciated by one skilled in the art in conjunction with the accompanying drawings, in which:

FIG. 1 is a schematic structure diagram of the data storage system used for the security information interaction according to the embodiment of the present invention; and

FIG. 2 is a flow diagram of the data storage method used for the security information interaction according to the embodiment of the present invention.

10 **Detailed description of the invention**

FIG. 1 is a schematic structure diagram of the data storage system used for the security information interaction according to the embodiment of the present invention. As shown in FIG. 1, the data storage system used for the security information interaction disclosed in the present invention comprises a security information storage device 1, an unlock password generating device 2 and an unlock server 3. Said security information storage device 1 is used to store and provide the data information related to the security information interaction. Said unlock password generating device 2 is used to generate the unlock password corresponding to said security information storage device 1 based on the original parameters extracted from said security information storage device 1, and to write said unlock password into said security information storage device 1. Said unlock server 3 is used to generate the unlock password corresponding to said security information storage device 1 based on the original parameters acquired from said security information storage device 1 when said security information storage device 1 is locked, and to use said unlock password to unlock said locked security information storage device 1.

Exemplarily, said original parameters are at least one factor being capable of uniquely identifying said security information storage device 1.

Exemplarily, said original parameters are the identifier (i.e., ID) of said security information storage device 1.

Exemplarily, said data information related to the security information interaction include an unlock password, a user password and business authentication data (e.g. a digital certificate, a dynamic password or the like).

As shown in FIG. 1, preferably, in the data storage system used for the security information interaction disclosed in the present invention, said security information storage device 1 further comprises a data communication interface 5, an unlock password initialization module 6, an unlock module 7, a locking module 8 and a data storage module 9. Said data communication interface 5 is used to complete the data communication with external devices. Said unlock password initialization module 6 is used to provide the original parameters corresponding to said security information storage device 1 in response to an original parameters extracting request message from said unlock password generating device 2, and to store the generated unlock password from said unlock password generating device 2 into said data storage module 9. Said unlock module 7 is used to provide the original parameters corresponding to said security information storage device 1 according to an original parameters extracting request message from said unlock server 3, and to unlock said security information storage device 1 based on the unlock password in the unlock request message from said unlock server 3. Said locking module 8 is used to lock said security information storage device 1 when a predetermined condition is satisfied (exemplarily, said predetermined condition is that the number of times that the error user passwords are entered continuously reaches a predetermined number of times). Said data storage module 9 is used to store said data information related to the security information interaction.

Optionally, in the data storage system used for the security information interaction disclosed in the present invention, said security information storage device 1 further comprises an information reset module 15. Said information reset

module 15 is used to initialize the predetermined items in said data information related to the security information interaction when said security information storage device 1 is unlocked (exemplarily, said predetermined items are user passwords).

5 Preferably, in the data storage system used for the security information interaction disclosed in the present invention, said data communication interface 5 is a USB interface.

As shown in FIG. 1, preferably, in the data storage system used for the security information interaction disclosed in the present invention, said unlock password
10 generating device 2 further comprises an original parameters extracting module 10 and a password generating module 11. Said original parameters extracting module 10 is used to send said original parameters extracting request message to said security information storage device 1, and to transmit the original parameters acquired from said security information storage device 1 to said password
15 generating module 11. Said password generating module 11 is used to generate an unlock password corresponding to said security information storage device 1 based on said original parameters and by means of invoking a first dynamic link library (key algorithm dynamic link library DLL1), and to transmit the generated unlock password to said security information storage device 1.

20 Preferably, in the data storage system used for the security information interaction disclosed in the present invention, said first dynamic link library is set by a service provider (e.g. a bank) or the relevant third party (i.e., said first dynamic link library is provided by a service provider or the relevant third party).

As shown in FIG. 1, preferably, in the data storage system used for the security
25 information interaction disclosed in the present invention, said unlock server 3 further comprises an original parameters acquiring module 12, an unlock password generating module 13 and an unlock initiating module 14. Said original parameters acquiring module 12 is used to send an original parameters extracting request message to said security information storage device 1, and to transmit the original

parameters acquired from said security information storage device 1 to said unlock password generating module 13. Said unlock password generating module 13 is used to generate an unlock password corresponding to said security information storage device 1 based on said original parameters and by means of invoking the
5 second dynamic link library (an unlock dynamic link library DLL2), and to transmit the generated unlock password to said unlock initiating module 14. Said unlock initiating module 14 is used to configure an unlock request message based on said generated unlock password, and to transmit said unlock request message to said security information storage device 1.

10 Preferably, in the data storage system used for the security information interaction disclosed in the present invention, said second dynamic link library is set by the manufacturer of said security information storage device 1 (i.e., said second dynamic link library is provided by the manufacturer of said security information storage device 1).

15 As shown in FIG. 1, exemplarily, in the data storage system used for the security information interaction disclosed in the present invention, said external devices include a user terminal 4, the unlock password generating device 2 and the unlock server 3.

Exemplarily, in the data storage system used for the security information
20 interaction disclosed in the present invention, said security information storage device 1 is a USBKey.

As shown in FIG. 1, the basic operational principle of the data storage system used for the security information interaction disclosed in the present invention is as follows: the manufacturer of said security information storage device 1 invokes
25 said first dynamic link library based on the original parameters extracted from said security information storage device 1 and by means of using the unlock password generating device 2, so as to generate an unlock password corresponding to said security information storage device 1, and to write said unlock password into said security information storage device 1; when said security information storage

device 1 is locked (for example, the number of times that the error user passwords are entered continuously reaches a predetermined number of times), said unlock server 3 invokes said second dynamic link library based on the original parameters acquired from said security information storage device 1, so as to
5 generate an unlock password corresponding to said security information storage device 1, and to use said unlock password to unlock said locked security information storage device 1; when said security information storage device 1 is in a non-locked state, said security information storage device 1 can communicate with said user terminal 4 via said data communication interface 5, so as to complete
10 the interaction of the security information related to businesses (for example, the authentication of the security data in the financial transaction).

FIG. 2 is a flow diagram of the data storage method used for the security information interaction according to the embodiment of the present invention. As shown in FIG. 2, the data storage method used for the security information
15 interaction disclosed in the present invention comprises the following steps: (A1) an unlock password generating device generating an unlock password corresponding to a security information storage device based on the original parameters extracted from said security information storage device, and writing said unlock password into said security information storage device; (A2) an unlock
20 server generating an unlock password corresponding to said security information storage device based on the original parameters acquired from said security information storage device when said security information storage device is locked, and using said unlock password to unlock said locked security information storage device; (A3) said security information storage device communicating with a user
25 terminal via a data communication interface when said security information storage device is in a non-locked state, so as to complete the interaction of the security information (for example, the authentication of the security data in the financial transaction).

Exemplarily, in the data storage method used for the security information

interaction disclosed in the present invention, said original parameters are at least one factor being capable of uniquely identifying said security information storage device.

Exemplarily, in the data storage method used for the security information
5 interaction disclosed in the present invention, said original parameters are the identifier (i.e., ID) of said security information storage device.

Exemplarily, in the data storage method used for the security information interaction disclosed in the present invention, said security information is business authentication data (e.g. a digital certificate, a dynamic password or the like).

10 As shown in FIG. 2, preferably, the data storage method used for the security information interaction disclosed in the present invention further comprises: (A4) locking said security information storage device when a predetermined condition is satisfied (exemplarily, said predetermined condition is that the number of times that the error user passwords are entered continuously reaches a
15 predetermined number of times).

As shown in FIG. 2, preferably, in the data storage method used for the security information interaction disclosed in the present invention, said step (A2) further comprises: initializing the predetermined items when said security information storage device is unlocked (exemplarily, said predetermined items are
20 user passwords).

Preferably, in the data storage method used for the security information interaction disclosed in the present invention, said data communication interface is a USB interface.

As shown in FIG. 2, preferably, in the data storage method used for the
25 security information interaction disclosed in the present invention, said step (A1) further comprises: (B1) sending an original parameters extracting request message to said security information storage device, so as to acquire the original parameters from said security information storage device; and (B2) generating an unlock password corresponding to said security information storage device based on said

original parameters and by means of invoking the first dynamic link library (key algorithm dynamic link library DLL1), and transmitting the generated unlock password to said security information storage device.

Preferably, in the data storage method used for the security information interaction disclosed in the present invention, said first dynamic link library is set by a service provider (e.g. a bank) or the relevant third party (i.e., said first dynamic link library is provided by a service provider or the relevant third party).

As shown in FIG. 2, preferably, in the data storage method used for the security information interaction disclosed in the present invention, said step (A2) further comprises: (C1) sending an original parameters extracting request message to said security information storage device, so as to acquire the original parameters from said security information storage device; (C2) generating an unlock password corresponding to said security information storage device based on said original parameters and by means of invoking the second dynamic link library (an unlock dynamic link library DLL2); and (C3) configuring an unlock request message based on the generated unlock password, and transmitting said unlock request message to said security information storage device.

Preferably, in the data storage method used for the security information interaction disclosed in the present invention, said second dynamic link library is set by the manufacturer of said security information storage device (i.e., said second dynamic link library is provided by the manufacturer of said security information storage device 1).

Exemplarily, in the data storage method used for the security information interaction disclosed in the present invention, said security information storage device is a USBKey.

Although the present invention is described by way of the preferred embodiments mentioned above, but its realization form is not limited to aforementioned embodiments. It should be recognized that various changes and modifications can be made to the present invention by one skilled in the art without

departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A data storage system used for the security information interaction, said data storage system used for the security information interaction comprising:

5 a security information storage device for storing and providing the data information related to the security information interaction;

an unlock password generating device for generating the unlock password corresponding to said security information storage device based on the original parameters extracted from said security information storage device, and writing
10 said unlock password into said security information storage device; and

an unlock server for generating the unlock password corresponding to said security information storage device based on the original parameters acquired from said security information storage device when said security information storage device is locked, and using said unlock password to unlock said locked security
15 information storage device.

2. The data storage system used for the security information interaction as claimed in claim 1, characterized in that, said original parameters are at least one factor being capable of uniquely identifying said security information storage device.

20 3. The data storage system used for the security information interaction as claimed in claim 2, characterized in that, said original parameters are the identifier of said security information storage device.

4. The data storage system used for the security information interaction as claimed in claim 3, characterized in that, said data information related to the
25 security information interaction include an unlock password, a user password and business authentication data.

5. The data storage system used for the security information interaction as claimed in claim 4, characterized in that, said security information storage device

further comprises:

a data communication interface for completing the data communication with external devices;

an unlock password initialization module for providing the original parameters
5 corresponding to said security information storage device in response to an original parameters extracting request message from said unlock password generating device, and storing the generated unlock password from the unlock password generating device into a data storage module;

an unlock module for providing the original parameters corresponding to said
10 security information storage device according to an original parameters extracting request message from said unlock server, and unlocking said security information storage device based on the unlock password in the unlock request message from said unlock server;

a locking module for locking said security information storage device when a
15 predetermined condition is satisfied; and

a data storage module for storing said data information related to the security information interaction.

6. The data storage system used for the security information interaction as claimed in claim 5, characterized in that, said security information storage device
20 further comprises an information reset module, said information reset module is used to initialize the predetermined items in said data information related to the security information interaction when said security information storage device is unlocked.

7. The data storage system used for the security information interaction as
25 claimed in claim 6, characterized in that, said data communication interface is a USB interface.

8. The data storage system used for the security information interaction as claimed in claim 7, characterized in that, said unlock password generating device further comprises:

an original parameters extracting module for sending said original parameters extracting request message to said security information storage device, and transmitting the original parameters acquired from said security information storage device to a password generating module; and

5 a password generating module for generating an unlock password corresponding to said security information storage device based on said original parameters and by means of invoking a first dynamic link library, and transmitting the generated unlock password to said security information storage device.

9. The data storage system used for the security information interaction as
10 claimed in claim 8, characterized in that, said first dynamic link library is set by a service provider or the relevant third party.

10. The data storage system used for the security information interaction as claimed in claim 9, characterized in that, said unlock server further comprises:

an original parameters acquiring module for sending an original parameters
15 extracting request message to said security information storage device, and transmitting the original parameters acquired from said security information storage device to an unlock password generating module;

an unlock password generating module for generating an unlock password
corresponding to said security information storage device based on said original
20 parameters and by means of invoking a second dynamic link library, and transmitting the generated unlock password to an unlock initiating module; and

an unlock initiating module for configuring an unlock request message based on the generated unlock password, and transmitting said unlock request message to said security information storage device.

25 11. The data storage system used for the security information interaction as claimed in claim 10, characterized in that, said second dynamic link library is set by the manufacturer of said security information storage device.

12. The data storage system used for the security information interaction as claimed in claim 11, characterized in that, said security information storage device

is an USBKey.

13. A data storage method used for the security information interaction, said data storage method used for the security information interaction comprising the following steps:

5 (A1) an unlock password generating device generating an unlock password corresponding to a security information storage device based on the original parameters extracted from said security information storage device, and writing said unlock password into said security information storage device;

(A2) an unlock server generating an unlock password corresponding to said
10 security information storage device based on the original parameters acquired from said security information storage device when said security information storage device is locked, and using said unlock password to unlock said locked security information storage device;

(A3) said security information storage device communicating with a user
15 terminal via a data communication interface when said security information storage device is in a non-locked state, so as to complete the interaction of the security information.

14. The data storage method used for the security information interaction as claimed in claim 13, characterized in that, said original parameters are at least one
20 factor being capable of uniquely identifying said security information storage device.

15. The data storage method used for the security information interaction as claimed in claim 14, characterized in that, said original parameters are the identifier of said security information storage device.

25 16. The data storage method used for the security information interaction as claimed in claim 15, characterized in that, said security information is business authentication data.

17. The data storage method used for the security information interaction as claimed in claim 16, characterized in that, said data storage method used for the

security information interaction further comprises:

(A4) locking said security information storage device when a predetermined condition is satisfied.

18. The data storage method used for the security information interaction as
5 claimed in claim 17, characterized in that, said step (A2) further comprises:
initializing the predetermined items when said security information storage device
is unlocked.

19. The data storage method used for the security information interaction as
claimed in claim 18, characterized in that, said data communication interface is a
10 USB interface.

20. The data storage method used for the security information interaction as
claimed in claim 19, characterized in that, said step (A1) further comprises:

(B1) sending an original parameters extracting request message to said
security information storage device, so as to acquire the original parameters from
15 said security information storage device; and

(B2) generating an unlock password corresponding to said security
information storage device based on said original parameters and by means of
invoking a first dynamic link library, and transmitting the generated unlock
password to said security information storage device.

21. The data storage method used for the security information interaction as
20 claimed in claim 20, characterized in that, said first dynamic link library is set by a
service provider or the relevant third party.

22. The data storage method used for the security information interaction as
claimed in claim 21, characterized in that, said step (A2) further comprises:

25 (C1) sending an original parameters extracting request message to said
security information storage device, so as to acquire the original parameters from
said security information storage device;

(C2) generating an unlock password corresponding to said security
information storage device based on said original parameters and by means of

invoking a second dynamic link library; and

(C3) configuring an unlock request message based on the generated unlock password, and transmitting said unlock request message to said security information storage device.

5 23. The data storage method used for the security information interaction as claimed in claim 22, characterized in that, said second dynamic link library is set by the manufacturer of said security information storage device.

24. The data storage method used for the security information interaction as claimed in claim 23, characterized in that, said security information storage device
10 is a USBKey.