

METHOD AND APPARATUS FOR REALIZING SWITCHING BETWEEN INTELLIGENT KEY DEVICE MODES

FIELD

5 The present disclosure relates to the computer technology field, and more particularly, to a method and an apparatus for switching modes of intelligent cipher token.

BACKGROUND

10 An electronic signature token (KEY) is a security device, provided with a single chip or an intelligent card chip. The electronic signature token has a certain storage space for storing a private key and a digital certificate of a user, and realizes the authentication of user's identity and the data encryption using a built-in public key algorithm. When applied in the financial business, the electronic signature token is mainly used for storing user certifications and signing transaction information, so as to realize the identity authentication when the user conducts a transaction on
15 network bank and ensure non-repudiation of the transaction.

 A one-time password (OTP) is an unpredictable combination of random digits generated according to a special algorithm. The one-time password is validate for one time, and mainly applied in a field such as network bank and used for protecting the user's transaction and login. The OTP may be applied in a terminal, such as a mobile phone, a tablet computer, etc. or may be
20 applied in a special hardware device.

 At present, functions of the KEY and the OTP may be incorporated into a same hardware device simultaneously. Although the functions of the KEY and the OTP can be implemented on a same carrier, the two functions are independent of each other, and it is inconvenient to switch therebetween.

25

SUMMARY

 Embodiments of the present disclosure seek to solve at least one of the problems described above.

 Accordingly, a first objective of the present disclosure is to provide a method for switching
30 modes of an intelligent cipher token. The method may realize the switching between a KEY mode and an OTP mode in a convenient and reliable way, such that the KEY and the OTP may be

incorporated physically and functions thereof may be integrated, thus saving cost and bringing convenience for users.

A second objective of the present disclosure is to provide another method for switching modes of an intelligent cipher token.

5 A third objective of the present disclosure is to provide yet another method for switching modes of an intelligent cipher token.

A fourth objective of the present disclosure is to provide an apparatus for switching modes of an intelligent cipher token.

10 A fifth objective of the present disclosure is to provide another apparatus for switching modes of an intelligent cipher token.

A sixth objective of the present disclosure is to provide yet another apparatus for switching modes of an intelligent cipher token.

In order to achieve the above objectives, embodiments of a first aspect of the present disclosure provide a method for switching modes of an intelligent cipher token, including:
15 switching the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode if the intelligent cipher token receives a switching instruction sent from a first button, after the intelligent cipher token establishes a connection with a terminal device via a first interface; in which the first mode is one of an electronic signature token (KEY) mode and an one-time password (OTP) mode, and the second mode is the other one of the KEY
20 mode and the OTP mode.

With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, after the intelligent cipher token establishes the connection with the terminal device via the first interface, the switching instruction sent from the first button is received and the intelligent cipher token is switched from the first mode which the intelligent
25 cipher token is currently in to the second mode, such that the switching between the KEY mode and the OTP mode may be realized in a convenient and reliable way and the KEY and the OTP may be integrated physically and functionally, thus saving cost and bringing convenience to users.

In order to achieve the above objectives, embodiments of a second aspect of the present disclosure provide another method for switching modes of an intelligent cipher token, including:
30 switching the intelligent cipher token from a current mode to a KEY mode when the intelligent cipher token detects that a connection status between a first interface and a terminal device is

changed from Unconnected to Connected, in which the current mode at least includes an OTP mode.

With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, after the intelligent cipher token detects that the connection status between the first interface and the terminal device is changed from Unconnected to Connected, the intelligent cipher token is switched from the current mode to the KEY mode, such that it is easy and convenient to switch modes of the intelligent cipher token, thus bringing convenience to users.

In order to achieve the above objectives, embodiments of a third aspect of the present disclosure provide yet another method for switching modes of an intelligent cipher token, including: switching the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode if the intelligent cipher token receives a switching instruction sent from a first button, after the intelligent cipher token establishes a connection with a terminal device via a first interface, in which the first mode is one of the KEY mode and the OTP mode, and the second mode is the other one of the KEY mode and the OTP mode; and switching the intelligent cipher token from a current mode to the KEY mode when the intelligent cipher token detects that a connection status between the first interface and the terminal device is changed from Unconnected to Connected, in which the current mode at least includes the OTP mode.

With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, by storing status information of two modes in an information structure of the intelligent cipher token, the switching between modes becomes more convenient, such that the KEY and the OTP may be integrated functionally and physically, thus saving cost and bringing convenience to users.

In order to achieve the above objectives, embodiments of a fourth aspect of the present disclosure provide an apparatus for switching modes of an intelligent cipher token, including: a first switching module, configured to receive a switching instruction sent from a first button and to switch the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode, after the intelligent cipher token establishes a connection with a terminal device via a first interface; in which the first mode is one of an electronic signature token (KEY) mode and an one-time password (OTP) mode, and the second mode is the other one of the KEY mode and the OTP mode.

In this embodiment of the present disclosure, the first switching module may receive the switching instruction sent from the first button and switch the intelligent cipher token from the first mode to the second mode.

When the intelligent cipher token is in the KEY mode, the first switching module may switch the intelligent cipher token to the OTP mode after receiving the switching instruction sent from the first button. Of course, when the intelligent cipher token is in the OTP mode, the first switching module may switch the intelligent cipher token to the KEY mode after receiving the switching instruction sent from the first button.

With the apparatus for switching modes of an intelligent cipher token according to embodiments of the present disclosure, after the intelligent cipher token establishes the connection with the terminal device via the first interface, the switching instruction sent from the first button is received and the intelligent cipher token is switched from the first mode which the intelligent cipher token is currently in to the second mode, such that the switching between the KEY mode and the OTP mode may be realized in a convenient and reliable way and the KEY and the OTP may be integrated physically and functionally, thus saving cost and bringing convenience to users.

In order to achieve the above objectives, embodiments of a fifth aspect of the present disclosure provide another apparatus for switching modes of an intelligent cipher token, including: a second switching module, configured to switch the intelligent cipher token from a current mode to a KEY mode if the intelligent cipher token detects that a connection status between a first interface and a terminal device is changed from Unconnected to Connected, in which the current mode at least includes an OTP mode.

When the connection status between the first interface of the intelligent cipher token and the terminal device is changed from Unconnected to Connected, the second switching module may switch the intelligent cipher token from the current mode to the KEY mode. For example, when the intelligent cipher token is a USBKEY and in a second OTP sub-mode, the USBKEY may be switched to the KEY mode automatically by only connecting the USBKEY to a host via a USB interface.

With the apparatus for switching modes of an intelligent cipher token according to embodiments of the present disclosure, after the intelligent cipher token detects that the connection status between the first interface and the terminal device is changed from Unconnected to Connected, the intelligent cipher token is switched from the current mode to the KEY mode, such

that it is easy and convenient to switch between modes of the intelligent cipher token, thus bringing convenience to users.

In order to achieve the above objectives, embodiments of a sixth aspect of the present disclosure provide yet another apparatus for switching modes of an intelligent cipher token, including: a first switching module, configured to switch the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode if the intelligent cipher token receives a switching instruction sent from a first button, after the intelligent cipher token establishes a connection with a terminal device via a first interface, in which the first mode is one of the KEY mode and the OTP mode, and the second mode is the other one of the KEY mode and the OTP mode; and a second switching module, configured to switch the intelligent cipher token from a current mode to the KEY mode if the intelligent cipher token detects that a connection status between the first interface and the terminal device is changed from Unconnected to Connected, in which the current mode at least includes the OTP mode.

With the apparatus for switching modes of an intelligent cipher token according to embodiments of the present disclosure, the switching between the modes may be realized conveniently and reliably, such that the KEY and the OTP may be integrated functionally and physically, thus saving cost and bringing convenience to users.

Additional aspects and advantages of embodiments of present disclosure will be given in part in the following descriptions, become apparent in part from the following descriptions, or be learned from the practice of the embodiments of the present disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a flow chart of a method for switching modes of an intelligent cipher token according to an example embodiment of the present disclosure;

Fig. 2 is a flow chart of a method for switching modes of an intelligent cipher token according to another example embodiment of the present disclosure;

Fig. 3 is a flow chart of a method for switching modes of an intelligent cipher token according to yet another example embodiment of the present disclosure;

Fig. 4 is a flow chart of a specific process for switching an intelligent cipher token from a first mode to a second mode according to an example embodiment of the present disclosure;

Fig. 5 is a flow chart of a method for switching modes of an intelligent cipher token

according to a specific embodiment of the present disclosure; and

Fig. 6 is a block diagram of an apparatus for switching modes of an intelligent cipher token according to an example embodiment of the present disclosure.

5 DETAILED DESCRIPTION

Embodiments of the present disclosure will be described in detail below. Examples of the embodiments are shown in the accompanying drawings in which the same or similar elements and the elements having same or similar functions are denoted by like reference numerals throughout the descriptions. The embodiments described herein with reference to drawings are explanatory,
10 illustrative, and used to generally understand the present disclosure. The embodiments shall not be construed to limit the present disclosure.

In the following, the method and the apparatus for switching modes of an intelligent cipher token according to embodiments of the present disclosure will be described with reference to drawings.

15 Fig. 1 is a flow chart of a method for switching modes of an intelligent cipher token according to an example embodiment of the present disclosure. In this embodiment, the intelligent cipher token may include a first mode and a second mode.

As shown in Fig. 1, the method for switching modes of an intelligent cipher token may include followings.

20 In act S101, the intelligent cipher token establishes a connection with a terminal device via a first interface.

In embodiments of the present disclosure, the intelligent cipher token may establish the connection with the terminal device via the first interface. The first interface may be a wired interface or a wireless interface. The wired interface may include a USB interface or an audio
25 interface. The wireless interface may include a Bluetooth interface, an infrared interface, an NFC interface or a WIFI interface, etc.

The intelligent cipher token may be a USBKEY, an audio KEY, a Bluetooth KEY, an infrared KEY, an NFCKEY or a WIFIKEY. If the intelligent cipher token is a USBKEY, the connection with the terminal device may be established via a USB interface. If the intelligent cipher token is
30 an audio KEY, the connection with the terminal device may be established via an audio interface. If the intelligent cipher token is a Bluetooth KEY, a Bluetooth module of the terminal device may

be started, and the connection with the terminal device may be established via a Bluetooth interface. If the intelligent cipher token is an infrared KEY, an infrared module of the terminal device may be started, and the connection with the terminal device may be established via an infrared interface. If the intelligent cipher token is an NFCKEY, an NFC module of the terminal device may be started, and the connection with the terminal device may be established via an NFC interface. If the intelligent cipher token is a WIFIKEY, a WIFI module of the terminal device may be started, and the connection with the terminal device may be established via a WIFI interface.

In act S102, a switching instruction sent from a first button is received by the intelligent cipher token.

In embodiments of the present disclosure, the intelligent cipher token may be provided with a first button. The first button may be a navigation key. The intelligent cipher token may receive the switching instruction sent from the first button after the intelligent cipher token establishes the connection with the terminal device via the first interface, such that the intelligent cipher token may be switched from the first mode where the intelligent cipher token is in to the second mode.

In act S103, the intelligent cipher token is switched from the first mode which the intelligent cipher token is currently in to the second mode.

In embodiments of the present disclosure, the intelligent cipher token may include two modes, i.e., the KEY mode and the OTP mode.

Specifically, when the intelligent cipher token is in the KEY mode, after the switching instruction sent from the first button is received, the intelligent cipher token may be switched to the OTP mode. Certainly, when the intelligent cipher token is in the OTP mode, after the switching instruction sent from the first button is received, the intelligent cipher token may be switched to the KEY mode.

It should be understood that, if the intelligent cipher token is connected with the terminal device via the first interface and in the OTP mode, the OTP mode is configured as a first OTP sub-mode.

In addition, the intelligent cipher token may include a dormant state and an awakened state. If the intelligent cipher token is in the first mode or the second mode, it may be considered that the intelligent cipher token is in the awakened state.

When the intelligent cipher token is connected with the terminal device via the first interface and in the first OTP sub-mode, the intelligent cipher token would enter the dormant state if

detecting that the first interface is disconnected from the terminal device.

With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, after the intelligent cipher token establishes the connection with the terminal device via the first interface, the switching instruction sent from the first button is received and the intelligent cipher token is switched from the first mode to the second mode, such that the switching between the KEY mode and the OTP mode may be realized in a convenient and reliable way and the KEY and the OTP may be integrated physically and functionally, thus saving cost and bringing convenience to users.

Fig. 2 is a flow chart of a method for switching modes of an intelligent cipher token according to another embodiment of the present disclosure.

As shown in Fig. 2, the method for switching modes of an intelligent cipher token may include followings.

In act S201, the intelligent cipher token detects that a connection status between a first interface and a terminal device is changed from Unconnected to Connected.

In embodiments of the present disclosure, the intelligent cipher token may be in the dormant state, and may enter the awakened state from the dormant state.

Specifically, the intelligent cipher token receives an awakening instruction. The awakening instruction comes from the first interface or a second button which may be a power key.

After receiving the awakening instruction, the intelligent cipher token may determine whether the awakening instruction is from the first interface. If the awakening instruction is not from the first interface, the intelligent cipher token determines that a connection with the terminal device is not established via the first interface, and determines whether the awakening instruction is from the second button. If the awakening instruction is from the second button, the intelligent cipher token enters the OTP mode.

It should be understood that, if the intelligent cipher token does not establish a connection with the terminal device via the first interface and is in the OTP mode, the OTP mode may be configured as a second OTP sub-mode.

In act S202, the intelligent cipher token is switched from a current mode to a KEY mode.

In embodiments of the present disclosure, when the connection status between the first interface of the intelligent cipher token and the terminal device is changed from Unconnected to Connected, the intelligent cipher token may be switched from the second OTP sub-mode which the

intelligent cipher token is currently in to the KEY mode. For example, if the intelligent cipher token is a USBKEY and in the second OTP sub-mode, the USBKEY may be switched to the KEY mode automatically by merely connecting the USBKEY to a host via a USB interface.

When the intelligent cipher token is in the KEY mode, the intelligent cipher token may enter the dormant state if detecting that the first interface is disconnected from the terminal device.

When the intelligent cipher token is in the second OTP sub-mode, the intelligent cipher token may enter the dormant state if detecting a trigger instruction from the second button.

With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, when it is determined that the intelligent cipher token detects that the connection status between the first interface and the terminal device is changed from Unconnected to Connected, the intelligent cipher token is switched from the current mode to the KEY mode, such that it is easy and convenient to switch modes of the intelligent cipher token, thus bringing convenience to users.

Fig. 3 is a flow chart of a method for switching modes of an intelligent cipher token according to yet another example embodiment of the present disclosure.

As shown in Fig. 3, the method for switching modes of an intelligent cipher token may include followings.

In act S301, an awakening instruction is received.

In embodiments of the present disclosure, the intelligent cipher token may be in the dormant state and may enter the awakened state from the dormant state.

In act S302, the dormant state is changed to the awakened state, it is determined whether the awakening instruction is from a first interface, if yes, the act at block S303 is executed; otherwise, the act at block S304 is executed.

In act S303, it is determined that the intelligent cipher token establishes a connection with a terminal device via the first interface, and the intelligent cipher token is switched to a KEY mode.

After receiving the awakening instruction, the intelligent cipher token may determine whether the awakening instruction is from the first interface. If the awakening instruction is from the first interface, it is determined that the intelligent cipher token establishes the connection with the terminal device via the first interface, and the intelligent cipher token is switched to the KEY mode, and then the act at block S305 may be executed to complete the switching between modes.

In act S304, it is determined that the intelligent cipher token does not establish the connection

with the terminal device via the first interface, and it is determined whether the awakening instruction is from a second button. If the awakening instruction is from the second button, the intelligent cipher token is switched to an OTP mode.

If the awakening instruction is not from the first interface, it is determined that the intelligent cipher token does not establish the connection with the terminal device via the first interface. Then, it is determined whether the awakening instruction is from the second button. If the awakening instruction is from the second button, the intelligent cipher token is switched to the OTP mode, and then the act at block S306 may be executed to complete the switching between modes.

The first interface may include a wired interface or a wireless interface. The wired interface may include a USB interface or an audio interface. The wireless interface may include a Bluetooth interface, an infrared interface, an NFC interface or a WIFI interface, etc. The intelligent cipher token may be a USBKEY, an audio KEY, a Bluetooth KEY, an infrared KEY, an NFCKEY or a WIFIKEY. If the intelligent cipher token is a USBKEY, the connection with the terminal device may be established via a USB interface. If the intelligent cipher token is an audio KEY, the connection with the terminal device may be established via an audio interface. If the intelligent cipher token is a Bluetooth KEY, a Bluetooth module of the terminal device may be started, and the connection with the terminal device may be established via a Bluetooth interface. If the intelligent cipher token is an infrared KEY, an infrared module of the terminal device may be started, and the connection with the terminal device may be established via an infrared interface. If the intelligent cipher token is an NFCKEY, an NFC module of the terminal device may be started, and the connection with the terminal device may be established via an NFC interface. If the intelligent cipher token is a WIFIKEY, a WIFI module of the terminal device may be started, and the connection with the terminal device may be established via a WIFI interface. The intelligent cipher token may further include a second button which may be a power key.

It should be understood that, the intelligent cipher token may be in a second OTP sub-mode or a dormant state, if the intelligent cipher token is not connected with the terminal device via the first interface.

In act S305, after determining that the intelligent cipher token establishes the connection with the terminal device via the first interface, the intelligent cipher token is switched from a first mode which the intelligent cipher token is currently in to a second mode if the intelligent cipher token receives a switching instruction sent from a first button. The first mode is one of the KEY mode

and the OTP mode, and the second mode is the other one of the KEY mode and the OTP mode.

In embodiments of the present disclosure, after the intelligent cipher token enters the KEY mode, the switching instruction sent from the first button may be received and then the intelligent cipher token may be switched to the OTP mode.

5 Of course, when the intelligent cipher token is in the OTP mode, the intelligent cipher token may be switched to the KEY mode after receiving the switching instruction sent from the first button.

It should be understood that, if the intelligent cipher token is connected with the terminal device via the first interface and in the OTP mode, the OTP mode is configured as a first OTP
10 sub-mode.

In embodiments of the present disclosure, when the intelligent cipher token is connected with the terminal device via the first interface and in the first OTP sub-mode, the intelligent cipher token enters the dormant state if detecting that the first interface is disconnected from the terminal device.

15 In act S306, when the intelligent cipher token detects that a connection status between the first interface and the terminal device is changed from Unconnected to Connected, the intelligent cipher token is switched from a current mode to the KEY mode. The current mode at least includes the OTP mode.

When the connection status between the first interface of the intelligent cipher token and the
20 terminal device is changed from Unconnected to Connected, the intelligent cipher token may be switched from the current mode to the KEY mode. For example, when the intelligent cipher token is a USBKEY and in the second OTP sub-mode, the intelligent cipher token may be switched to the KEY mode automatically by merely connecting the USBKEY to a host via a USB interface. When the intelligent cipher token is in the KEY mode, the intelligent cipher token may enter the
25 dormant state if detecting that the first interface is disconnected from the terminal device. When the intelligent cipher token is in the second OTP sub-mode, the intelligent cipher token enters the dormant state if detecting a trigger instruction from a second button.

In embodiments of the present disclosure, after determining that the intelligent cipher token establishes the connection with the terminal device via the first interface, the act at block S305
30 may be executed to switch the intelligent cipher token from the first mode which the intelligent cipher token is currently in to the second mode. As shown in Fig. 4, the specific process may be

explained as follows.

In act S3051, the intelligent cipher token receives a switching instruction sent from a first button.

The first button may be a navigation key.

5 In act S3052, the intelligent cipher token reads out first status information and first check information storing in an information structure.

In act S3053, the intelligent cipher token performs a cyclic redundancy check (CRC) calculation on the first status information to obtain a first check value.

10 In act S3054, the intelligent cipher token compares the first check value with the first check information. If the first check value is the same as the first check information, the act at block S3055 is executed.

In act S3055, the intelligent cipher token performs the CRC calculation on second status information to obtain second check information. The second status information is status information of the intelligent cipher token in the current working mode.

15 The intelligent cipher token may store the second status information and the second check information into the information structure, and configure the second status information as the first status information and the second check information as the first check information.

In act S3056, the intelligent cipher token performs a switching operation, so as to switch from the first mode to the second mode.

20 Specifically, the switching operation may be performed by a skip or a soft reset. The skip refers to that a program goes to a specific position to execute codes. The soft reset refers to that the CPU is reset via instructions.

25 Thus, it can be seen that, the switching between the first OTP sub-mode and the KEY mode is caused by an operation on a menu bar by a user, and it is required to store information of the intelligent cipher token into the information structure to complete the mode switching. However, the switching from the second OTP sub-mode to the KEY mode is caused by a change of hardware signal, the mode switching may be realized without the information structure.

30 In embodiments of the present disclosure, the information structure is stored in the intelligent cipher token. On one hand, after the state of the intelligent cipher token is switched, information stored in the information structure may be read, such that the intelligent cipher token may continue to perform the operations before the last switching, without re-processing data before the

switching; on the other hand, since data stored in the information structure may be incorrect due to the change of external working environment, information storing in the information structure may be checked so as to prevent the intelligent cipher token from processing the incorrect data read out from the information structure, such that the switching between modes may be realized reliably.

5 With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, by storing status information of two modes in an information structure of the intelligent cipher token, the switching between modes becomes more convenient, such that the KEY and the OTP may be integrated functionally and physically, thus saving cost and bringing convenience to users.

10 Fig. 5 is a flow chart of a method for switching modes of an intelligent cipher token according to a specific embodiment of the present disclosure. In this embodiment, assume that the intelligent cipher token is a USBKEY, the first interface is a USB interface and the terminal is a PC, and illustration is made based on such an example.

15 As shown in Fig. 5, the method for switching modes of an intelligent cipher token may include followings.

 In act S501, the intelligent cipher token is in an initial state.

 Specifically, the initial state may be a dormant state with low power consumption, and the intelligent cipher token may be awakened via an external signal.

20 In act S502, it is determined whether the USB interface is connected to the terminal device, if yes, the act at block S503 is executed, i.e., the intelligent cipher token enters the KEY mode; or else, that act at block S504 is executed, i.e., it is determined whether to awaken the intelligent cipher token via a power key.

 In act S503, the intelligent cipher token enters the KEY mode, and then the act at block S506 is executed via a navigation key.

25 In act S504, it is determined whether the intelligent cipher token is awakened via the power key, if yes, the act at block S505 is executed; or else, the act at block S501 is executed, i.e., the intelligent cipher token goes back to the initial state.

 In act S505, the intelligent cipher token enters a second OTP sub-mode.

30 After the intelligent cipher token enters the second OTP sub-mode, the act at block S501 may be executed via a power-off key, i.e., the intelligent cipher token goes back to the initial state; or the act at block S503 may be executed by connecting the intelligent cipher token to the terminal

device via the USB interface, i.e., the intelligent cipher token enters the KEY mode. When the intelligent cipher token enters the KEY mode, working current may be provided via the USB interface. If the intelligent cipher token is in a power shortage state, the intelligent cipher token may be charged via the USB interface.

- 5 After the intelligent cipher token enters the KEY mode, the intelligent cipher token is disconnected from the terminal device, and the act S501 is executed, i.e., the intelligent cipher token goes back to the initial state.

 In act S506, the intelligent cipher token enters a first OTP sub-mode.

- After the intelligent cipher token enters the KEY mode, there is a choice to switch to the first
10 OTP sub-mode via the navigation key. After the intelligent cipher token enters the first OTP sub-mode, the working current may be provided via the USB interface. If the intelligent cipher token is in the power shortage state, the intelligent cipher token may be charged via the USB interface. Similarly, the act at block S503 is executed via the navigation key, i.e., the intelligent cipher token is switched to the KEY mode.

- 15 When the intelligent cipher token is in the KEY mode, the user may press down the navigation key, and the intelligent cipher token may provide navigation information on a display interface, such that the user may select to enter the OTP mode according to the navigation information and confirm that. The intelligent cipher token may be switched to the OTP mode after receiving a trigger request indicating a confirmation of entering the OTP mode. In this case, the
20 intelligent cipher token is switched from the KEY mode to the first OTP sub-mode.

- Specifically, the interface cipher token has an information structure stored therein. The information structure is configured to store status information and check information of the KEY mode or the OTP mode. When the switching between these two modes is performed via the navigation key, the information structure may be updated. Specifically, status information of the
25 current mode may be obtained from the information structure, and then the CRC calculation may be performed on the status information to obtain a check value. The obtained check value is compared with the pre-stored check information, if they are the same, then a switching operation is performed. After the state is switched, the intelligent cipher token may continue with operations to be performed before the switching by reading out information stored in the information structure,
30 without re-processing data previous to the switching.

 In addition, since the information stored in the information structure may be incorrect due to

the change of external working environment, it is required to check whether the information storing in the information structure is correct, so as to prevent the intelligent cipher token from processing the incorrect information. When the intelligent cipher token is switched from the KEY mode to the first OTP sub-mode via the navigation key, the status information of the KEY mode is stored firstly, and then the switching operation is performed via a skip or a soft reset. The skip refers to that a program goes to a specific position to execute codes. The soft reset refers to that the CPU is reset via instructions.

Certainly, after the intelligent cipher token enters the first OTP sub-mode, the intelligent cipher token may be switched to the KEY mode via the navigation key.

After the intelligent cipher token enters the first OTP sub-mode, the intelligent cipher token may be switched to the initial state by disconnecting the intelligent cipher token from the terminal device.

It can be seen that, the intelligent cipher token may enter the second OTP sub-mode via a power key. When detecting the USB interface is inserted into the terminal device, the intelligent cipher token may be switched from the second OTP sub-mode to the KEY mode. The intelligent cipher token may enter the first OTP sub-mode from the KEY mode through a menu selection, and may go back to the KEY mode through a menu selection.

Thus, the switching between the second OTP sub-mode and the KEY mode is caused by the change of hardware signal, and the switching between the first OTP sub-mode and the KEY mode is caused by an operation on the menu bar by the user. Further, for the switching between the first OTP sub-mode and the KEY mode, when the USB interface connects to the PC, the intelligent cipher token may enter the first OTP sub-mode. However, for the switching between the second OTP sub-mode and the KEY mode, when the USB interface connects to the PC, the intelligent cipher token may not enter the OTP mode (i.e., the intelligent cipher token can only enter the KEY mode).

With the method for switching modes of an intelligent cipher token according to embodiments of the present disclosure, the switching between the KEY mode and the OTP mode may be realized conveniently and reliably, such that the KEY and the OTP may be integrated functionally and physically, thus saving cost and bringing convenience to users. Further, since the intelligent cipher token stores the information structure, it is more convenient to switch between modes by storing status information of the two modes.

In order to implement above embodiments, the present disclosure further provide an apparatus for switching modes of an intelligent cipher token.

According to an embodiment of the present disclosure, there is provided an apparatus for switching modes of an intelligent cipher token (not shown in drawings), the apparatus includes a
5 first switching module.

The first switching module is configured to receive a switching instruction sent from a first button and to switch the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode, after the intelligent cipher token establishes a connection with a terminal device via a first interface. The first mode is one of the KEY mode and the OTP
10 mode, and the second mode is the other one of the KEY mode and the OTP mode.

The intelligent cipher token may be a USBKEY, an audio KEY, a Bluetooth KEY, an infrared KEY, an NFCKEY or a WIFIKEY. If the intelligent cipher token is a USBKEY, the connection with the terminal device may be established via a USB interface. If the intelligent cipher token is an audio KEY, the connection with the terminal device may be established via an audio interface.
15 If the intelligent cipher token is a Bluetooth KEY, a Bluetooth module of the terminal device may be started, and the connection with the terminal device may be established via a Bluetooth interface. If the intelligent cipher token is an infrared KEY, an infrared module of the terminal device may be started, and the connection with the terminal device may be established via an infrared interface. If the intelligent cipher token is an NFCKEY, an NFC module of the terminal
20 device may be started, and the connection with the terminal device may be established via an NFC interface. If the intelligent cipher token is a WIFIKEY, a WIFI module of the terminal device may be started, and the connection with the terminal device may be established via a WIFI interface.

In embodiments of the present disclosure, the first switching module may receive a switching instruction sent from the first button and switch the intelligent cipher token from the first mode to
25 the second mode.

When the intelligent cipher token is in the KEY mode, the first switching module may switch the intelligent cipher token to the OTP mode after receiving the switching instruction sent from the first button. Certainly, when the intelligent cipher token is in the OTP mode, the first switching module may switch the intelligent cipher token to the KEY mode after receiving the switching
30 instruction sent from the first button.

With the apparatus for switching modes of an intelligent cipher token according to

embodiments of the present disclosure, the switching between the KEY mode and the OTP mode may be realized in a convenient and reliable way, such that the KEY and the OTP may be integrated physically and functionally, thus saving cost and bringing convenience to users.

According to another embodiment of the present disclosure, there is provided an apparatus for switching modes of an intelligent cipher token (not shown in drawings), the apparatus includes a second switching module.

The second switching module is configured to switch the intelligent cipher token from a current mode to a KEY mode when the intelligent cipher token detects that a connection status between a first interface and a terminal device is changed from Unconnected to Connected, in which the current mode at least includes an OTP mode.

The intelligent cipher token may be a USBKEY, an audio KEY, a Bluetooth KEY, an infrared KEY, an NFCKEY or a WIFIKEY. If the intelligent cipher token is a USBKEY, the connection with the terminal device may be established via a USB interface. If the intelligent cipher token is an audio KEY, the connection with the terminal device may be established via an audio interface. If the intelligent cipher token is a Bluetooth KEY, a Bluetooth module of the terminal device may be started, and the connection with the terminal device may be established via a Bluetooth interface. If the intelligent cipher token is an infrared KEY, an infrared module of the terminal device may be started, and the connection with the terminal device may be established via an infrared interface. If the intelligent cipher token is an NFCKEY, an NFC module of the terminal device may be started, and the connection with the terminal device may be established via an NFC interface. If the intelligent cipher token is a WIFIKEY, a WIFI module of the terminal device may be started, and the connection with the terminal device may be established via a WIFI interface.

When the connection status between the first interface of the intelligent cipher token and the terminal device is changed from Unconnected to Connected, the second switching module may switch the intelligent cipher token from the current mode to the KEY mode. For example, if the intelligent cipher token is a USBKEY and in a second OTP sub-mode, the intelligent cipher token may be switched to the KEY mode automatically by merely connecting the intelligent cipher token to a host via a USB interface.

With the apparatus for switching modes of an intelligent cipher token according to embodiments of the present disclosure, the switching between the KEY mode and the OTP mode may be realized in a convenient and reliable way, such that the KEY and the OTP may be

integrated physically and functionally, thus saving cost and bringing convenience to users.

Fig. 6 is a block diagram of an apparatus for switching modes of an intelligent cipher token according to an example embodiment of the present disclosure.

As shown in Fig. 6, the apparatus includes a first switching module 61 and a second
5 switching module 62.

The first switching module 61 is configured to receive a switching instruction sent from a first button and to switch the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode, after determining that the intelligent cipher token establishes a connection with a terminal device via a first interface. The first mode is one of the
10 KEY mode and the OTP mode, and the second mode is the other one of the KEY mode and the OTP mode.

In embodiments of the present disclosure, the first switching module 61 may receive the switching instruction sent from a first button, and switch the intelligent cipher token from the first mode which the intelligent cipher token is currently in to the second mode. Specifically, the first
15 switching module 61 receives the switching instruction sent from the first button, reads out first status information and first checks information in an information structure, performs a CRC calculation on the first status information to obtain a first check value, compares the first check value with the first check information. If the first check value is the same as the first check information, then the first switching module 61 performs a CRC calculation on second status
20 information (status information of the intelligent cipher token in a current working mode) to obtain second check information, and performs a switching operation by a skip or a soft reset to switch from the first mode to the second mode. The intelligent cipher token may store the second status information and the second check information into the information structure, and configures the second status information as the first status information and the second check information as the
25 first check information.

When the intelligent cipher token is in the KEY mode, the intelligent cipher token may be switched to the OTP mode after the first switching module 61 receives the switching instruction sent from the first button. Certainly, when the intelligent cipher token is in the OTP mode, the intelligent cipher token may be switched to the KEY mode after the first switching module 61
30 receives the switching instruction sent from the first button.

The second switching module 62 is configured to switch the intelligent cipher token from a

current mode to the KEY mode when the intelligent cipher token detects that a connection status between the first interface and the terminal device is changed from Unconnected to Connected, in which the current mode at least includes an OTP mode.

When the connection status between the first interface of the intelligent cipher token and the terminal device is changed from Unconnected to Connected, the second switching module 62 may switch the intelligent cipher token from the current mode to the KEY mode. For example, if the intelligent cipher token is a USBKEY and in a second OTP sub-mode, the intelligent cipher token may be switched to the KEY mode automatically by merely connecting the intelligent cipher token to a host via a USB interface.

In addition, the apparatus further includes a processing module 63.

The processing module 63 is configured to receive an awakening instruction; to enable the intelligent cipher token to enter an awakened state from a dormant state; to determine whether the awakening instruction is from the first interface; to determine that the intelligent cipher token establishes the connection with the terminal device via the first interface and to enable the intelligent cipher token to enter the KEY mode, if the awakening instruction is from the first interface; to determine that the intelligent cipher token does not establish the connection with the terminal device via the first interface and to determine whether the awakening instruction is from a second button, if the awakening instruction is not from the first interface; and to enable the intelligent cipher token to enter the OTP mode if the awakening instruction is from the second button.

Further, the apparatus for switching modes of an intelligent cipher token may further include a dormancy module 64.

The dormancy module 64 is configured to enable the intelligent cipher token to enter the dormant state when detecting the first interface is disconnected from the terminal device, after it is determined that the intelligent cipher token is connected to the terminal device via the first interface and the intelligent cipher token is in the OTP mode. The dormancy module 64 is further configured to enable the intelligent cipher token to enter the dormant state when detecting the first interface is disconnected from the terminal device, after it is determined that the intelligent cipher token is connected to the terminal device via the first interface and the intelligent cipher token is in the KEY mode. The dormancy module 64 is further configured to receive a trigger instruction from a second button, and to enable the intelligent cipher token to enter the dormant state when

detecting the trigger instruction from the second button, after it is determined that the intelligent cipher token is connected to the terminal device via the first interface and the intelligent cipher token is in the OTP mode.

Concerning the process of realizing the switching between modes of the intelligent cipher token, reference may be made to the method embodiments shown in Figs. 1-4, which are not described herein.

With the apparatus for switching modes of an intelligent cipher token according to embodiments of the present disclosure, the switching between the KEY mode and the OTP mode may be realized in a convenient and reliable way, such that the KEY and the OTP may be integrated physically and functionally, thus saving cost and bringing convenience to users.

Reference throughout this specification to “an embodiment,” “some embodiments,” “one embodiment,” “another example,” “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. Thus, the appearances of the phrases such as “in some embodiments,” “in one embodiment,” “in an embodiment,” “in another example,” “in an example,” “in a specific example,” or “in some examples,” in various places 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.

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. Thus, the feature defined with “first” and “second” may comprise one or more this feature. In the description of the present disclosure, “a plurality of” means two or more than two, unless specified otherwise.

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

The logic and/or step described in other manners herein or shown in the flow chart, for example, a particular sequence table of executable instructions for realizing the logical function, may be specifically achieved in any computer readable medium to be used by the instruction
5 execution system, device or equipment (such as the system based on computers, the system comprising processors or other systems capable of obtaining the instruction from the instruction execution system, device and equipment and executing the instruction), or to be used in combination with the instruction execution system, device and equipment. As to the specification, “the computer readable medium” may be any device adaptive for including, storing,
10 communicating, propagating or transferring programs to be used by or in combination with the instruction execution system, device or equipment. More specific examples of the computer readable medium comprise but are not limited to: an electronic connection (an electronic device) with one or more wires, a portable computer enclosure (a magnetic device), a random access memory (RAM), a read only memory (ROM), an erasable programmable read-only memory
15 (EPROM or a flash memory), an optical fiber device and a portable compact disk read-only memory (CDROM). In addition, the computer readable medium may even be a paper or other appropriate medium capable of printing programs thereon, this is because, for example, the paper or other appropriate medium may be optically scanned and then edited, decrypted or processed with other appropriate methods when necessary to obtain the programs in an electric manner, and
20 then the programs may be stored in the computer memories.

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, a plurality of 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
25 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. 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 method for switching modes of an intelligent cipher token, wherein the intelligent cipher token comprises a first button and a first interface, and the method comprises:

5 switching the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode if the intelligent cipher token receives a switching instruction sent from the first button, after the intelligent cipher token establishes a connection with a terminal device via the first interface, wherein the first mode is one of a KEY mode and an OTP mode, and the second mode is the other one of the KEY mode and the OTP mode; and

10 switching the intelligent cipher token from a current mode to the KEY mode when the intelligent cipher token detects that a connection status between the first interface and the terminal device is changed from Unconnected to Connected, wherein the current mode at least comprises the OTP mode.

2. The method according to claim 1, wherein, the first interface comprises a wired interface or
15 a wireless interface, in which the wired interface comprises a universal serial bus (USB) interface or an audio interface, and the wireless interface comprises a Bluetooth interface, an infrared interface, a near field wireless communication (NFC) interface or a wireless fidelity (WIFI) interface.

3. The method according to claim 1 or 2, wherein the intelligent cipher token further
20 comprises a second button, and the method further comprises:

receiving, by the intelligent cipher token, an awakening instruction;

enabling the intelligent cipher token to enter an awakened state from a dormant state, determining whether the awakening instruction is from the first interface;

determining that the intelligent cipher token establishes the connection with the terminal
25 device via the first interface and enabling the intelligent cipher token to enter the KEY mode, if the awakening instruction is from the first interface;

determining that the intelligent cipher token does not establish the connection with the terminal device via the first interface and determining whether the awakening instruction is from the second button, if the awakening instruction is not from the first interface; and

30 enabling the intelligent cipher token to enter the OTP mode, if the awakening instruction is from the second button.

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

enabling the intelligent cipher token to enter a dormant state if detecting the first interface is disconnected from the terminal device, after it is determined that the intelligent cipher token establishes the connection with the terminal device via the first interface and the intelligent cipher token is in the OTP mode.

5. The method according to claim 1 or 2, wherein switching the intelligent cipher token from a first mode to a second mode if the intelligent cipher token receives a switching instruction sent from the first button comprises:

A, receiving, by the intelligent cipher token, the switching instruction sent from the first button;

B, reading out, by the intelligent cipher token, first status information and first check information storing in an information structure;

C, performing, by the intelligent cipher token, a cyclic redundancy check (CRC) calculation on the first status information so as to obtain a first check value;

D, comparing, by the intelligent cipher token, the first check value with the first check information, and executing act E if the first check value is the same as the first check information;

E, performing, by the intelligent cipher token, a cyclic redundancy check CRC calculation on second status information so as to obtain second check information, wherein the second status information is status information of the intelligent cipher token in the current mode; storing, by the intelligent cipher token, the second status information and the second check information into the information structure, and configuring the second status information as the first status information and configuring the second check information as the first check information; and

F, performing, by the intelligent cipher token, a switching operation to switch from the first mode to the second mode.

6. The method according to claim 5, wherein, the switching operation comprises a switching operation by skip, or a switching operation by soft reset.

7. The method according to any one of claims 1, 2 and 6, wherein the OTP mode comprises a first OTP sub-mode and a second OTP sub-mode; if it is determined that the intelligent cipher token establishes the connection with the terminal device via the first interface, the OTP mode where the intelligent cipher token is in is configured as the first OTP sub-mode; if it is determined that the intelligent cipher token does not establish the connection with the terminal device via the

first interface, the OTP mode where the intelligent cipher token is in is configured as the second OTP sub-mode.

8. An apparatus for switching modes of an intelligent cipher token, wherein the intelligent cipher token comprises a first button and a first interface, and the apparatus comprises:

5 a first switching module, configured to switch the intelligent cipher token from a first mode which the intelligent cipher token is currently in to a second mode if the intelligent cipher token receives a switching instruction sent from the first button, after the intelligent cipher token establishes a connection with a terminal device via the first interface, wherein the first mode is one of a KEY mode and an OTP mode, and the second mode is the other one of the KEY mode and the
10 OTP mode; and

a second switching module, configured to switch the intelligent cipher token from a current mode to the KEY mode when the intelligent cipher token detects that a connection status between the first interface and the terminal device is changed from Unconnected to Connected, wherein the current mode at least comprises the OTP mode.

15 9. The apparatus according to claim 8, wherein, the first interface comprises a wired interface or a wireless interface, in which the wired interface comprises a universal serial bus (USB) interface or an audio interface, and the wireless interface comprises a Bluetooth interface, an infrared interface, a near field wireless communication (NFC) interface or a wireless fidelity (WIFI) interface.

20 10. The apparatus according to claim 8 or 9, the intelligent cipher token further comprises a second button, and the apparatus further comprises:

a processing module, configured to:

receive an awakening instruction;

enable the intelligent cipher token to enter an awakened state from dormant state, and

25 determine whether the awakening instruction is from the first interface;

determine that the intelligent cipher token establishes the connection with the terminal device via the first interface and enable the intelligent cipher token to enter the KEY mode, if the awakening instruction is from the first interface;

30 determine that the intelligent cipher token does not establish the connection with the terminal device via the first interface and determine whether the awakening instruction is from the second button, if the awakening instruction is not from the first interface; and

enable the intelligent cipher token to enter the OTP mode, if the awakening instruction is from the second button.

11. The apparatus according to claim 8 or 9, further comprising:

5 a dormancy module, configured to enable the intelligent cipher token to enter a dormant state if detecting the first interface is disconnected from the terminal device, after it is determined that the intelligent cipher token establishes the connection with the terminal device via the first interface and the intelligent cipher token is in the OTP mode.

12. The apparatus according to claim 8 or 9, wherein the first switching module is configured to:

10 receive the switching instruction sent from the first button;
read out first status information and first check information storing in an information structure;

perform a cyclic redundancy check (CRC) calculation on the first status information so as to obtain a first check value;

15 compare the first check value with the first check information;

if the first check value is the same as the first check information, perform a cyclic redundancy check CRC calculation on second status information so as to obtain second check information, wherein the second status information is status information of the intelligent cipher token in the current mode; store the second status information and the second check information into the
20 information structure, and configure the second status information as the first status information and configure the second check information as the first check information; and

perform a switching operation to switch from the first mode to the second mode.

13. The apparatus according to claim 12, wherein, the switching operation comprises a switching operation by skip, or a switching operation by soft reset.

25 14. The apparatus according to any one of claims 8, 9 and 13, wherein, the OTP mode comprises a first OTP sub-mode and a second OTP sub-mode; if it is determined that the intelligent cipher token establishes the connection with the terminal device via the first interface, the OTP mode where the intelligent cipher token is in is configured as the first OTP sub-mode; if it is determined that the intelligent cipher token does not establish the connection with the terminal
30 device via the first interface, the OTP mode where the intelligent cipher token is in is configured as the second OTP sub-mode.

15. A computer-readable storage medium having stored therein computer instructions that, when executed, causes the method for switching modes of an intelligent cipher token according to any one of claims 1-7 to be performed.