METHOD FOR INFORMATION SECURITY EQUIPMENT TO REALIZE MULTIPLE APPLICATIONS, INFORMATION SECURITY EQUIPMENT AND SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

This application is based upon and claims a priority to Chinese Patent Application Serial No. 201410072040.7, filed with the State Intellectual Property Office of P. R. China on February 28, 2014 by TENDYRON CORPORATION, and entitled "a method for realizing a plurality of applications in an information security device, an information security device and system for realizing a plurality of applications", the entire contents of which are incorporated herein by reference.

FIELD

The present disclosure generally relates to the electronic technology field, and more particularly to a method for realizing a plurality of applications in an information security device, an information security device and an information security system.

BACKGROUND

With the rapid development of Internet technology and e-commerce, information security issues become serious increasingly, such that various information security devices configured to protect users' sensitive information are produced. These devices, by coordinating with a PKI (Public Key Infrastructure) system, can ensure various information security operations effectively, for example, users' data interaction, information identification and authority management, etc.

However, one information security device in the related art is usually configured to realize only one function. If the user wants to realize various functions, he or she needs to purchase various information security devices, which are complicated to use and inconvenient to carry. Meanwhile, the function supported by the information security device is usually fixed and cannot be upgraded or be added. If the user wants to use a new function or an upgraded function, he or she needs to purchase a new information security device again, which will increase the user's usage cost.

SUMMARY

The present disclosure provides a method for realizing a plurality of applications in an information security device, an information security device for realizing a plurality of applications and an information security system for realizing a plurality of applications, so as to at least solve the problem in the related art that one information security device cannot support a plurality of applications.

According to an aspect of the present disclosure, there is provided a method for realizing a plurality of applications in an information security device, including: compiling, by a terminal, a written application program to obtain an intermediate code file corresponding to the written application program; performing, by the terminal, a security verification on the intermediate code file; storing, by the terminal, an intermediate code file passing the security verification; receiving, by the terminal, a request for downloading application programs sent by the information security device; obtaining, by the terminal, at least two intermediate code files corresponding to two application programs requested to be downloaded according to the request for downloading application programs; sending, by the terminal, the at least two intermediate code files corresponding to two application programs to the information security device; receiving and storing, by the information security device, the at least two intermediate code files corresponding to two application programs; receiving, by the information security device, a first executive command; and executing, by an intermediate code interpreter in the information security device, an intermediate code file corresponding to an application program indicated by the first executive command, in which the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

In addition, data storage spaces in the information security device are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

In addition, before receiving by the information security device a first executive command, the method further includes: receiving, by the information security device, a first activating instruction; and activating, by the information security device, an intermediate code file corresponding to an application program indicated by the first activating instruction; in which executing by an intermediate code interpreter in the information security device an intermediate code file corresponding to an application program indicated by the first executive command specifically includes: executing, by the intermediate code interpreter in the information security device, an activated intermediate code file corresponding to the application program indicated by

the first executive command.

In addition, during a process of executing by the intermediate code interpreter in the information security device the intermediate code file corresponding to the application program indicated by the first executive command, if a data access request is generated by the intermediate code file corresponding to the application program indicated by the first executive command, the method further includes: judging, by the intermediate code interpreter, whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command; if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, allowing, by the intermediate code interpreter, the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access; and if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command, refusing, by the intermediate code interpreter, to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access.

According to another aspect of the present disclosure, there is provided an information security device for realizing a plurality of applications, including: a sending module, configured to send a request for downloading application programs to a terminal; a receiving module, configured to receive from the terminal at least two intermediate code files corresponding to two application programs requested to be downloaded, and to receive a first executive command, in which the at least two intermediate code files corresponding to two application programs are obtained by the terminal by compiling written application programs and performing security verifications; a storage module, configured to store the at least two intermediate code files corresponding to two application programs; and an intermediate code interpreter, configured to execute an intermediate code file corresponding to an application program indicated by the first executive command, in which the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

In addition, data storage spaces in the storage module are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

In addition, the receiving module is further configured to receive a first activating instruction;

the information security device further includes: an activating module, configured to activate an intermediate code file corresponding to an application program indicated by the first activating instruction; the intermediate code interpreter is specifically configured to execute an activated intermediate code file corresponding to the application program indicated by the first executive command.

In addition, the intermediate code interpreter is further configured to judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, to allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and to refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.

According to yet another aspect of the present disclosure, there is provided an information security system for realizing a plurality of applications, including: a terminal, configured to compile a written application program to obtain an intermediate code file corresponding to the written application program, to perform a security verification on the intermediate code file, to store an intermediate code file passing the security verification, to receive a request for downloading application programs sent by an information security device, to obtain at least two intermediate code files corresponding to two application programs requested to be downloaded according to the request for downloading application programs, and to send the at least two intermediate code files corresponding to two application programs to the information security device; and the information security device, configured to send the request for downloading application programs to the terminal, to receive and store the at least two intermediate code files corresponding to two application programs, to receive a first executive command, in which an intermediate code interpreter in the information security device is configured to execute an intermediate code file corresponding to an application program indicated by the first executive command, and the intermediate code file is configured to call an application program interface of

the information security device to control hardware of the information security device.

In addition, data storage spaces in the information security device are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

In addition, the information security device is further configured to receive a first activating instruction, and to activate an intermediate code file corresponding to an application program indicated by the first activating instruction; the intermediate code interpreter in the information security device is specifically configured to execute an activated intermediate code file corresponding to the application program indicated by the first executive command.

In addition, the intermediate code interpreter in the information security device is further configured to judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, to allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and to refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.

According to still another aspect of the present disclosure, there is provided an information security device for realizing a plurality of applications, including: one or more processors; a memory; one or more programs stored in the memory, in which when being executed by the one or more processors, the one or more programs are configured to: send a request for downloading application programs to a terminal; receive from the terminal at least two intermediate code files corresponding to two application programs requested to be downloaded, in which the at least two intermediate code files corresponding to two application programs are obtained by the terminal by compiling written application programs and performing security verifications; store the at least two intermediate code files corresponding to two application programs; receive a first executive command; and execute an intermediate code file corresponding to an application program indicated by the first executive command, in which the intermediate code file is configured to call an application program interface of the information security device to control hardware of the

information security device.

In addition, data storage spaces are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

In addition, when being executed by the one or more processors, the one or more programs are further configured to: receive a first activating instruction; activate an intermediate code file corresponding to an application program indicated by the first activating instruction; the one or more programs are further configured to execute an intermediate code file corresponding to an application program indicated by the first executive command by a step of executing an activated intermediate code file corresponding to the application program indicated by the first executive command.

In addition, when being executed by the one or more processors, the one or more programs are further configured to: judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command; allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.

It can be seen from the above technical solutions provided by the present disclosure that, the present disclosure provides the method for realizing a plurality of applications in an information security device, the information security device for realizing a plurality of applications and the information security system for realizing a plurality of applications. The information security device may download the intermediate code file corresponding to the application (or application program) from the terminal, and the intermediate code interpreter is used to execute the intermediate code file to call the system application program interface (API) to control the hardware, such that the plurality of applications may be realized in the information security device and the application may be updated dynamically. Under considerations of system security, the application program is converted into the executable intermediate code file, and the intermediate

code interpreter (located inside an operating system of the information security device) is used to execute the intermediate code file corresponding to the application program, i.e. the application program runs on the virtual machine instead of operating the hardware directly. More rigorous inspection and judgment may be performed on the intermediate code file by the virtual machine, such that illegal operations (such as array bound, type mismatch, etc.) are rejected and the application program is isolated from the hardware, thereby improving portability of application program and compatibility of hardware. In addition, the operating system defines the API, which facilitates the development and functional expansion of application programs, thereby improving the development efficiency of application programs.

BRIEF DESCRIPTION OF THE DRAWINGS

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

Fig. 1 is a flow chart illustrating a method for realizing a plurality of applications in an information security device provided by Embodiment One of the present disclosure;

Fig. 2 is a block diagram illustrating an information security device for realizing a plurality of applications provided by Embodiment Two of the present disclosure; and

Fig. 3 is a block diagram illustrating an information security system for realizing a plurality of applications provided by Embodiment Three of the present disclosure.

DETAILED DESCRIPTION

The technique solution in embodiments of the present disclosure will be described in the following with reference to drawings in the embodiments of the present disclosure. Obviously, the embodiments to be described only are some embodiments of the present disclosure, instead of all the embodiments thereof. Based on embodiments of the present disclosure, other embodiments obtained by those having ordinary skills in the related art without making creative labors fall into a protection scope of the present disclosure. 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.

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

Embodiment One

The embodiment provides a method for realizing a plurality of applications in an information security device. In this embodiment, a terminal may be a personal computer (PC), and the information security device may be an intelligent cipher key token (for example, a USB key, an audio key, etc.). By adopting the method provided in this embodiment of the present disclosure, the information security device may realize various applications besides the signature function.

Fig. 1 is a flow chart illustrating a method for realizing a plurality of applications in an information security device provided by Embodiment One of the present disclosure. As illustrated in Fig. 1, the method includes the following steps 101 to 109.

In step 101, the terminal compiles a written application program to obtain an intermediate code file corresponding to the written application program.

The application program may be written in high-level languages, for example, BASIC language, True BASIC language, PASCAL language, FORTRAN language, C language or C ++ language, Java language, etc. The application program may be compiled and converted into the intermediate code file corresponding to the application program by tools on terminal-side. The intermediate code file is executable intermediate codes and in a format of machine-like language which is between source language and machine language. The intermediate code file may be executed by an intermediate code interpreter in the information security device.

For example, if the application program is written in Java language. The terminal may compile and convert the application program written in Java language into the executable intermediate code file using a compilation and conversion tool, for example, the intermediate code file may be Java byte codes.

In step 102, the terminal performs a security verification on the intermediate code file. The terminal may ensure the accuracy of intermediate code file by performing the security verification on the intermediate code file and further ensure that the intermediate code interpreter in the information security device can execute the intermediate code file normally after the information security device downloads the intermediate code file, so as to realize functions supported by the application program corresponding to the intermediate code file, and to increase the security of the

information security device.

In step 103, the terminal stores an intermediate code file passing the security verification.

The terminal may process a plurality of different application programs according to the above steps 101 and 102, so as to obtain intermediate code files corresponding to the plurality of different application programs.

The terminal may store the intermediate code files corresponding to the plurality of application programs so as to be downloaded by the information security device.

In step 104, the terminal receives a request for downloading application programs sent by the information security device.

If the information security device needs to download a plurality of application programs, then a plurality of requests for downloading application programs may be sent, in which one request is configured to download one application program; or one request may be sent to request downloading the plurality of application programs. In at least one embodiment, an identifier of the application program to be downloaded may be carried in the request for downloading application program.

In step 105, the terminal obtains at least two intermediate code files corresponding to two application programs requested to be downloaded according to the request for downloading application programs.

In step 106, the terminal sends the at least two intermediate code files corresponding to two application programs to the information security device.

In step 107, the information security device receives and stores the at least two intermediate code files corresponding to two application programs.

During the process of downloading the intermediate code file corresponding to the application program described in step 104 to step 107, the terminal may send the at least two intermediate code files corresponding to two application programs to the information security device via a wireless communication interface, for example, a Bluetooth interface, an NFC interface, an infrared interface etc.; or the terminal may send the at least two intermediate code files corresponding to two application programs to the information security device via a wired connection communication interface, for example, a serial interface, a USB interface, an audio interface etc. The information security device may be provided with an application manager for managing application programs and completing operations, for example, downloading, deleting or

updating an application, etc. When the application program is updated, an updated intermediate code file may be downloaded from the terminal.

It should be noted that, after receiving the request for downloading application programs from the information security device, the terminal may compile and convert the written application program into the intermediate code file corresponding to the application program, perform the security verification on the intermediate code file, store the intermediate code file if the intermediate code file passes the security verification and then send the intermediate code file to the information security device.

In step 108, the information security device receives a first executive command.

The first executive command may be an instruction inputted by a user via a button. The button may be a physical key in a form of hardware, a virtual button displayed on a touch screen, or a module implementing the key function in other forms. The first executive command may also be sent by the terminal. For example, the user may select the application program via the button in the information security device, or the user may select the application program on the terminal, and then the terminal sends the executive command to the information security device.

In step 109, an intermediate code interpreter in the information security device executes an intermediate code file corresponding to an application program indicated by the first executive command, in which the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device. The system API of the information security device encapsulates system functions of standard information security applications, for example, encryption functions, decryption functions, display functions, button operating functions, external communication functions, etc. By using the system API, the development difficulty of application programs may be reduced and the development efficiency of application programs may be improved. The hardware of the information security device may be a button, a display, a Flash etc.

The intermediate code interpreter is located in an operating system of the information security device. When executing the intermediate code file (that is, the application program corresponding to the intermediate code file runs on the information security device), the intermediate code interpreter controls the hardware of the information security device by calling the system API of the information security device, and realizes operations, for example, encryption and decryption, displaying, data storage, external communications etc., so as to realize functions of application

programs in the information security device.

It can be seen from the above technical solutions that, the information security device in the embodiment may download the intermediate code file corresponding to the application (or application program) from the terminal, and the intermediate code interpreter is used to execute the intermediate code file to call the system application program interface (API) to control the hardware, such that the plurality of applications may be realized in the information security device and the application may be updated dynamically. Under considerations of system security, the application program is converted into the executable intermediate code file, and the intermediate code interpreter (located inside the operating system of the information security device) is used to execute the intermediate code file corresponding to the application program, i.e. the application program runs on the virtual machine instead of operating the hardware directly. More rigorous inspection and judgment may be performed on the intermediate code file by the virtual machine, such that illegal operations (such as array bound, type mismatch, etc.) are rejected and the application program is isolated from the hardware, thereby improving portability of application program and compatibility of hardware. In addition, the operating system defines the API, which facilitates the development and functional expansion of the application programs, thereby improving the development efficiency of the application programs.

Data storage spaces in the information security device configured to store the at least two intermediate code files corresponding to two application programs are in isolation. Each application program in the information security device has separate data storage, which guarantees the data isolation between application programs, thereby improving security. Further, the information security device may use separate data storage spaces to store the operating system and the application program respectively so as to isolate the data of the operating system from that of the application program, thereby further enhancing the security.

Before the information security device receives the first executive command in step 108, the method further includes following steps of: receiving, by the information security device, a first activating instruction; and activating, by the information security device, an intermediate code file corresponding to an application program indicated by the first activating instruction; in which executing by an intermediate code interpreter in the information security device an intermediate code file corresponding to an application program indicated by the first executive command specifically includes: executing, by the intermediate code interpreter in the information security

device, an activated intermediate code file corresponding to the application program indicated by the first executive command. In at least one embodiment, the user may activate the application in the information security device by selecting the application command, and the operating system distinguishes the application to be activated via an application identifier (AID). After the application is activated, the information security device is managed by the activated application and the activated application realizes corresponding security operation procedure.

During a process of executing by the intermediate code interpreter in the information security device the intermediate code file corresponding to the application program indicated by the first executive command, if a data access request is generated by the intermediate code file corresponding to the application program indicated by the first executive command, the method further includes: judging, by the intermediate code interpreter, whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command; if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, allowing, by the intermediate code interpreter, the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access; and if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command, refusing, by the intermediate code interpreter, to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access. In at least one embodiment, when the intermediate code interpreter judges whether the data requested to be accessed is authorized for the intermediate code file, the judgment may be performed by the application identifier. The data authorized for the intermediate code file belongs to the application's own data. When the application is running, the intermediate code interpreter checks whether the data to be accessed belongs to the application, if yes, the access may be allowed, and if no, the access may be refused and an error notification may be returned. In this way, security may be ensured and the user is instructed to handle in time in case of error.

By combining the specific examples, description of the above method is given in detail as follows.

The information security device supporting the signature application and the dynamic

verification application is taken as examples. The terminal compiles and converts the signature application and the dynamic verification application into intermediate code files corresponding respectively thereto, performs the security verification and stores the intermediate code files passing the security verification so as to be downloaded by the information security device.

The information security device sends the request for downloading the intermediate code file corresponding to the signature application and the request for downloading the intermediate code file corresponding to the dynamic verification application to the terminal, and uses separate storage spaces to store two applications respectively, activates the applications and waits for the executive command to use the corresponding application.

If the user wants to use the signature function of the information security device for online transaction, he or she may select the signature application corresponding to the signature function in the information security device. The intermediate code interpreter in the information security device may interpret and execute the intermediate code file corresponding to the signature application, and call the system API to control the hardware. First an external communication function is called to control the information security device to receive a transaction information sent by a transaction terminal (for example, a mobile phone, a personal computer, a tablet computer, etc.), and a display function is called to control the display screen to display the received transaction information for the user to confirm. After the user confirms, an encryption function is called to control the security chip to perform the signature on the transaction information, and the external communication function is called to control the information security device to transmit the signature data to the transaction terminal, and the transaction terminal verifies the received signature data via a server and completes the transaction if it is verified successfully.

If the user wants to use the dynamic verification application of the information security device for completing a transaction, he or she may select the dynamic verification application corresponding to the dynamic verification function in the information security device. The intermediate code interpreter in the information security device may interpret and execute the intermediate code file corresponding to the dynamic verification application, and call the system API to control the hardware. First the external communication function is called to control the information security device to receive a challenge code sent by the transaction terminal (for example, a mobile phone, a personal computer, a tablet computer, etc.) or a challenge code

inputted by the user via the button, and the encryption function is called to control the security chip to calculate a dynamic password according to the challenge code. The transaction terminal receives the dynamic password inputted by the user via the button and completes the verification via the server and further completes the transaction.

Embodiment Two

The embodiment provides an information security device for realizing a plurality of applications that may implement the operations executed by the information security device in the method described in Embodiment One. As shown in Fig. 2, the information security device includes a sending module 21, a receiving module 22, a storage module 23 and an intermediate code interpreter 24.

The sending module 21 is configured to send a request for downloading application programs to a terminal.

The receiving module 22 is configured to receive from the terminal at least two intermediate code files corresponding to two application programs requested to be downloaded, in which the at least two intermediate code files corresponding to two application programs are obtained by the terminal by compiling written application programs and performing security verifications.

The storage module 23 is connected with the receiving module 22 and is configured to store the at least two intermediate code files corresponding to two application programs received by the receiving module 22.

The receiving module 22 is further configured to receive a first executive command.

The intermediate code interpreter 24 is connected with the receiving module 22 and is configured to execute an intermediate code file corresponding to an application program indicated by the first executive command, which is received by the receiving module 22, in which the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

In addition, data storage spaces in the storage module 23 are configured to store the at least two intermediate code files corresponding to two application programs in isolation. Each application program in the information security device has separate data storage, which guarantees the data isolation between application programs, thereby improving security. Further, the information security device may use separate data storage spaces to store the operating system and the application program respectively so as to isolate the data of the operating system from that of

the application program, thereby further enhancing security.

The receiving module 22 is further configured to receive a first activating instruction; the above information security device further includes: an activating module, connected with the receiving module 22 and configured to activate an intermediate code file corresponding to an application program indicated by the first activating instruction, which is received by the receiving module 22; the intermediate code interpreter 24 is specifically configured to execute an activated intermediate code file corresponding to the application program indicated by the first executive command.

The intermediate code interpreter 24 is further configured to judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, to allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and to refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command. The data authorized for the intermediate code file belongs to the application's own data. When the application is running, the intermediate code interpreter checks whether the data to be accessed belongs to the application, if yes, the access may be allowed, and if no, the access may be refused and an error notification may be returned. In this way, security may be ensured and the user is instructed to handle in time in case of error.

It can be seen from the above technical solutions that, the information security device in the embodiment may download the intermediate code file corresponding to the application (or application program) from the terminal, and the intermediate code interpreter is used to execute the intermediate code file to call the system application program interface (API) to control the hardware, such that the plurality of applications may be realized in the information security device and the application may be updated dynamically. Under considerations of system security, the application program is converted into the executable intermediate code file, and the intermediate code interpreter (located inside the operating system of the information security device) is used to

execute the intermediate code file corresponding to the application program, i.e. the application program runs on the virtual machine instead of operating the hardware directly. More rigorous inspection and judgment may be performed on the intermediate code file by the virtual machine, such that illegal operations (such as array bound, type mismatch, etc.) are rejected and the application program is isolated from the hardware, thereby improving portability of application program and compatibility of hardware. In addition, the operating system defines the API, which facilitates the development and functional expansion of the application programs, thereby improving the development efficiency of the application programs.

Certainly, the above module division is only a schematic division and the present disclosure is not limited thereto. As long as the module division may realize the purposes of the present disclosure, it should belong to the scope of the present disclosure.

Embodiment Three

The embodiment provides an information security system for realizing a plurality of applications that may implement the operations executed by the information security device in the method described in Embodiment One. As shown in Fig. 3, the system includes an information security device 20 and a terminal 30, and the information security device 20 may be the information security device described in Embodiment Two.

The terminal 30, is configured to compile a written application program to obtain an intermediate code file corresponding to the written application program, to perform a security verification on the intermediate code file, to store an intermediate code file passing the security verification, to receive a request for downloading application programs sent by the information security device 20, to obtain at least two intermediate code files corresponding to two application programs requested to be downloaded according to the request for downloading application programs, and to send the at least two intermediate code files corresponding to two application programs to the information security device 20. The application to be downloaded by the information security device 20 may be pre-stored in the terminal. The terminal needs not repeat to write, compile, convert, verify and store each time when the application is downloaded.

The information security device 20 is configured to send the request for downloading application programs to the terminal 30, to receive and store the at least two intermediate code files corresponding to two application programs sent by the terminal 30, to receive a first executive command, in which an intermediate code interpreter in the information security device 20 is

configured to execute an intermediate code file corresponding to an application program indicated by the first executive command, and the intermediate code file is configured to call an application program interface of the information security device 20 to control hardware of the information security device 20.

In addition, data storage spaces in the information security device 20 are configured to store the at least two intermediate code files corresponding to two application programs in isolation. Each application program in the information security device has separate data storage, which guarantees the data isolation between application programs, thereby improving security. Further, the information security device may use separate data storage spaces to store the operating system and the application program respectively so as to isolate the data of the operating system from that of the application program, thereby further enhancing security.

In addition, the information security device 20 is further configured to receive a first activating instruction, and to activate an intermediate code file corresponding to an application program indicated by the first activating instruction; the intermediate code interpreter in the information security device 20 is specifically configured to execute an activated intermediate code file corresponding to the application program indicated by the first executive command.

In addition, the intermediate code interpreter in the information security device 20 is further configured to judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, to allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and to refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command. The data authorized for the intermediate code file belongs to the application's own data. When the application is running, the intermediate code interpreter checks whether the data to be accessed belongs to the application, if yes, the access may be allowed, and if no, the access may be refused and an error notification may be returned. In this way, security may be ensured and the user is

instructed to handle in time in case of error.

The information security device in the embodiment may be an intelligent cipher key token, for example, a USB key, a key supporting an audio interface, a key supporting a Bluetooth interface/ NFC Interface/WIFI, etc. or may also be an electronic/dynamic token, or may also a device integrated with a key and an electronic/dynamic token.

It can be seen from the above technical solutions that, the information security device in the embodiment may download the intermediate code file corresponding to the application (or application program) from the terminal, and the intermediate code interpreter is used to execute the intermediate code file to call the system application program interface (API) to control the hardware, such that the plurality of applications may be realized in the information security device and the application may be updated dynamically. Under considerations of system security, the application program is converted into the executable intermediate code file, and the intermediate code interpreter (located inside the operating system of the information security device) is used to execute the intermediate code file corresponding to the application program, i.e. the application program runs on the virtual machine instead of operating the hardware directly. More rigorous inspection and judgment may be performed on the intermediate code file by the virtual machine, such that illegal operations (such as array bound, type mismatch, etc.) are rejected and the application program is isolated from the hardware, thereby improving portability of application program and compatibility of hardware. In addition, the operating system defines the API, which facilitates the development and functional expansion of the application programs, thereby improving the development efficiency of the application programs.

Embodiment Four

The embodiment also provides an information security device for realizing a plurality of applications that may implement the operations executed by the information security device in the method described in Embodiment One. The information security device includes one or more processors, a memory, and one or more programs stored in the memory, in which when being executed by the one or more processors, the one or more programs are configured to perform the following steps S101' to S105'.

In step S101', a request for downloading application programs is sent to a terminal.

In step S102', at least two intermediate code files corresponding to two application programs requested to be downloaded are received from the terminal, in which the at least two intermediate

code files corresponding to two application programs are obtained by the terminal by compiling written application programs and performing security verifications.

In step S103', the at least two intermediate code files corresponding to two application programs are stored.

Data storage spaces are configured to store the at least two intermediate code files corresponding to the at least two application programs in isolation.

In S104', a first executive command is received.

In S105', an intermediate code file corresponding to an application program indicated by the first executive command is executed, in which the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

Before a first executive command is received in step S104', and when being executed by the one or more processors, the one or more programs are further configured to: receive a first activating instruction; activate an intermediate code file corresponding to an application program indicated by the first activating instruction. The one or more programs are further configured to execute an intermediate code file corresponding to an application program indicated by the first executive command by executing an activated intermediate code file corresponding to the application program indicated by the first executive command.

During a process of executing by the intermediate code interpreter in the information security device the intermediate code file corresponding to the application program indicated by the first executive command, if a data access request is generated by the intermediate code file corresponding to the application program indicated by the first executive command, and when being executed by the one or more processors, the one or more programs are further configured to: judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command; allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed

is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.

Any procedure or method described in the flow charts or described in any other way herein may be understood to comprise one or more modules, portions or parts for storing executable codes that realize particular logic functions or procedures. Moreover, advantageous embodiments of the present disclosure comprises 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 which embodiments of the present disclosure belong to.

It is 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 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.

It would be understood by those skilled in the art that all or a part of the steps carried by the method in the above-described embodiments may be completed by relevant hardware instructed by a program. The program may be stored in a computer readable storage medium. When the program is executed, one or a combination of the steps of the method in the above-described embodiments may be completed.

In addition, individual functional units in the embodiments of the present disclosure may be integrated in one processing module or may be separately physically present, or two or more units may be integrated in one module. The integrated module as described above may be achieved in the form of hardware, or may be achieved in the form of a software functional module. If the integrated module is achieved in the form of a software functional module and sold or used as a separate product, the integrated module may also be stored in a computer readable storage medium.

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

etc.

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

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

WHAT IS CLAIMED IS:

1. A method for realizing a plurality of applications in an information security device, comprising:

compiling, by a terminal, a written application program to obtain an intermediate code file corresponding to the written application program;

performing, by the terminal, a security verification on the intermediate code file;

storing, by the terminal, the intermediate code file passing the security verification;

receiving, by the terminal, a request for downloading application programs sent by the information security device;

obtaining, by the terminal, at least two intermediate code files corresponding to two application programs requested to be downloaded according to the request for downloading application programs;

sending, by the terminal, the at least two intermediate code files corresponding to two application programs to the information security device;

receiving and storing, by the information security device, the at least two intermediate code files corresponding to two application programs;

receiving, by the information security device, a first executive command; and

executing, by an intermediate code interpreter in the information security device, an intermediate code file corresponding to an application program indicated by the first executive command, wherein the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

2. The method according to claim 1, wherein data storage spaces in the information security device are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

3. The method according to claim 1 or 2, before receiving by the information security device the first executive command, further comprising:

receiving, by the information security device, a first activating instruction; and

activating, by the information security device, an intermediate code file corresponding to an application program indicated by the first activating instruction;

wherein executing by an intermediate code interpreter in the information security device an intermediate code file corresponding to an application program indicated by the first executive command specifically comprises: executing, by the intermediate code interpreter in the information security device, the activated intermediate code file corresponding to the application program indicated by the first executive command.

4. The method according to any one of claims 1 to 3, wherein

during a process of executing by the intermediate code interpreter in the information security device the intermediate code file corresponding to the application program indicated by the first executive command, if a data access request is generated by the intermediate code file corresponding to the application program indicated by the first executive command, the method further comprises:

judging, by the intermediate code interpreter, whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command;

if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, allowing, by the intermediate code interpreter, the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access; and

if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command, refusing, by the intermediate code interpreter, to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access.

5. An information security device for realizing a plurality of applications, comprising:

a sending module, configured to send a request for downloading application programs to a terminal;

a receiving module, configured to receive from the terminal at least two intermediate code files corresponding to two application programs requested to be

downloaded, and to receive a first executive command, wherein the at least two intermediate code files corresponding to two application programs are obtained by the terminal by compiling written application programs and performing security verifications;

a storage module, configured to store the at least two intermediate code files corresponding to two application programs, and

an intermediate code interpreter, configured to execute an intermediate code file corresponding to an application program indicated by the first executive command, wherein the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

6. The information security device according to claim 5, wherein data storage spaces in the storage module are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

7. The information security device according to claim 5 or 6, wherein

the receiving module is further configured to receive a first activating instruction;

the information security device further comprises:

an activating module, configured to activate an intermediate code file corresponding to an application program indicated by the first activating instruction;

the intermediate code interpreter is specifically configured to execute the activated intermediate code file corresponding to the application program indicated by the first executive command.

8. The information security device according to any one of claims 5 to 7, wherein

the intermediate code interpreter is further configured to judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, to allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and to refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if

the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.

9. An information security system for realizing a plurality of applications, comprising:

a terminal, configured to compile a written application program to obtain an intermediate code file corresponding to the written application program, to perform a security verification on the intermediate code file, to store the intermediate code file passing the security verification, to receive a request for downloading application programs sent by an information security device, to obtain at least two intermediate code files corresponding to two application programs requested to be downloaded according to the request for downloading application programs, and to send the at least two intermediate code files corresponding to two application programs to the information security device; and

the information security device, configured to send the request for downloading application programs to the terminal, to receive and store the at least two intermediate code files corresponding to two application programs, to receive a first executive command, wherein an intermediate code interpreter in the information security device is configured to execute an intermediate code file corresponding to an application program indicated by the first executive command, and the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

10. The information security system according to claim 9, wherein data storage spaces in the information security device are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

11. The information security system according to claim 9 or 10, wherein

the information security device is further configured to receive a first activating instruction, and to activate an intermediate code file corresponding to an application program indicated by the first activating instruction;

the intermediate code interpreter in the information security device is specifically configured to execute the activated intermediate code file corresponding to the application program indicated by the first executive command.

12. The information security system according to any one of claims 9 to 11, wherein

the intermediate code interpreter in the information security device is further configured to judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, to allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and to refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.

13. An information security device for realizing a plurality of applications, comprising:

one or more processors;

a memory;

one or more programs stored in the memory, wherein when being executed by the one or more processors, the one or more programs are configured to:

send a request for downloading application programs to a terminal;

receive from the terminal at least two intermediate code files corresponding to two application programs requested to be downloaded, wherein the at least two intermediate code files corresponding to two application programs are obtained by the terminal by compiling written application programs and performing security verifications;

store the at least two intermediate code files corresponding to two application programs;

receive a first executive command; and

execute an intermediate code file corresponding to an application program indicated by the first executive command, wherein the intermediate code file is configured to call an application program interface of the information security device to control hardware of the information security device.

14. The information security device according to claim 13, wherein data storage spaces are configured to store the at least two intermediate code files corresponding to two application programs in isolation.

15. The information security device according to claim 13 or 14, wherein when being executed by the one or more processors, the one or more programs are further configured to:

receive a first activating instruction; and

activate an intermediate code file corresponding to an application program indicated by the first activating instruction;

the one or more programs are further configured to execute an intermediate code file corresponding to an application program indicated by the first executive command by a step of executing the activated intermediate code file corresponding to the application program indicated by the first executive command.

16. The information security device according to any one of claims 13 to 15, wherein when being executed by the one or more processors, the one or more programs are further configured to:

judge whether data requested to be accessed by the intermediate code file corresponding to the application program indicated by the first executive command is authorized for the intermediate code file corresponding to the application program indicated by the first executive command;

allow the intermediate code file corresponding to the application program indicated by the first executive command to execute a data access if the data requested to be accessed is authorized for the intermediate code file corresponding to the application program indicated by the first executive command, and refuse to let the intermediate code file corresponding to the application program indicated by the first executive command execute a data access if the data requested to be accessed is not authorized for the intermediate code file corresponding to the application program indicated by the first executive command.