

DESCRIPTION

PORTABLE ELECTRONIC DEVICE AND IC CARD

FIELD

5 An embodiment of the present invention relates to a portable electronic device and an IC card.

BACKGROUND

Conventionally, a processing system including an IC card as a portable electronic device and an IC card
10 processing device is issued and processed so as to perform a specific process by a preset processing method according to an operation policy of the system. For example, the IC card is issued and processed so as to perform a cryptographic process by a single preset cryptographic
15 method. On the other hand, in recent years, in order to cope with the appearance of computers having advanced computing power such as quantum computers, cryptographic processing using a new cryptographic method such as quantum-resistant cryptography has been desired in a lot of
20 situations. In the conventional processing system described above, in order to perform a cryptographic process by a new cryptographic method such as quantum-resistant cryptography, not only the IC card but also all IC card processing devices need to be simultaneously replaced with
25 those adaptable to the new cryptographic method.

However, it is considered to be practically difficult to replace all IC cards and IC card processing devices in

the entire processing system in operation with those
adaptable to the new cryptographic method. Therefore, in
order to shift the cryptographic method used for
cryptographic processing from the existing one to the new
5 one, it is assumed that a transition period in which the
existing cryptographic method and the new one coexist as a
cryptographic method for performing a cryptographic process
is required. In such a transition period, it is desired
that the IC cards not only support both the existing and
10 new cryptographic methods, but also smoothly perform a
cryptographic process by a cryptographic method required by
the IC card processing devices.

CITATION LIST

PATENT LITERATURE

15 Patent literature 1: Jpn. Pat. Appln. KOKAI Publication No.
2020-10396

SUMMARY

TECHNICAL PROBLEM

In order to solve the above problem, the present
20 invention provides a portable electronic device and an IC
card which are capable of executing a specific process by
selecting one from among a plurality of processing methods.

SOLUTION TO PROBLEM

According to an embodiment, an interface a memory and
25 a processor. The interface communicates with an external
device. The memory stores setting information for each of a
plurality of different processing methods to perform a

specific process. The processor selects one of the processing methods to perform the specific process in accordance with information supplied from the external device, and performs the specific process by the selected one of the processing methods.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing a configuration example of an IC card as a portable electronic device according to an embodiment.

FIG. 2 is a block diagram showing a configuration example of an IC card processing device that communicates with the IC card as a portable electronic device according to the embodiment.

FIG. 3 is a diagram showing an example of storing setting information (setting flag) for each of a plurality of cryptographic methods in an NVM of the IC card as a portable electronic device according to the embodiment.

FIG. 4 is a diagram showing an example of storing information (identification flag) indicating a cryptographic method that is being selected (set) in a RAM of the IC card as a portable electronic device according to the embodiment.

FIG. 5 is a flowchart illustrating a first operation example of the IC card as a portable electronic device according to the embodiment.

FIG. 6 is a flowchart illustrating a second operation example of the IC card as a portable electronic device

according to the embodiment.

FIG. 7 is a flowchart illustrating a third operation example of the IC card as a portable electronic device according to the embodiment.

5 FIG. 8 is a flowchart illustrating a fourth operation example of the IC card as a portable electronic device according to the embodiment.

FIG. 9 is a flowchart illustrating a fifth operation example of the IC card as a portable electronic device
10 according to the embodiment.

FIG. 10 is a flowchart illustrating a sixth operation example of the IC card as a portable electronic device according to the embodiment.

FIG. 11 is a diagram showing a configuration example
15 of a signature verification command supplied to the IC card as a portable electronic device according to the embodiment.

FIG. 12 is a flowchart illustrating a seventh
operation example of the IC card as a portable electronic
20 device according to the embodiment.

FIG. 13 is a diagram showing an example of a signature verification command including a parameter that specifies a cryptographic method supplied to the IC card as a portable electronic device according to the embodiment.

25 FIG. 14 is a diagram showing an example of a signature verification command including a parameter that specifies a cryptographic method supplied to the IC card as a portable

electronic device according to the embodiment.

FIG. 15 is a flowchart illustrating a flow of an eighth operation example of the IC card as a portable electronic device according to the embodiment.

5 FIG. 16 is a diagram showing an example of a signature verification command for each cryptographic method supplied to the IC card as a portable electronic device according to the embodiment.

10 FIG. 17 is a diagram showing an example of a signature verification command for each cryptographic method supplied to the IC card as a portable electronic device according to the embodiment.

DETAILED DESCRIPTION

15 An embodiment will be described below with reference to the drawings.

20 FIG. 1 is a block diagram schematically showing a configuration example of an IC card 1 according to an embodiment. An IC card 1 as a portable electronic device according to the embodiment constitutes an IC card processing system together with an IC card processing device 2 as an external device. The IC card 1 is a portable electronic device that is activated (that is brought into an operable state) by electric power applied from the IC card processing device 2. The IC card 1 is also referred to
25 as a smart card.

 Note that the portable electronic device according to the embodiment is not limited to a card-shaped one but may

be a booklet-shaped one (e.g., a notebook such as a passport) having the same structure and processing function as the IC card 1 to be described later. The portable electronic device according to the embodiment may also be a portable electronic device (e.g., a smartphone, a mobile phone, a tablet PCs and a dongle) having the same structure and processing function as the IC card 1 to be described later.

The IC card 1 is roughly divided into a contact IC card and a non-contact IC card. The contact IC card 1 is activated by receiving an operation power supply and an operation clock from the IC card processing device 2 through a contact portion as a communication interface. For example, the contact IC card 1 is an IC card that conforms to a standard defined in ISO/IEC7816-3. The non-contact IC card 1 is activated by receiving radio waves from the IC card processing device 2 via an antenna and a modulation/demodulation circuit as a communication interface to generate an operation power supply and an operation clock from the radio waves. For example, the non-contact IC card 1 is an IC card that conforms to a standard defined in ISO/IEC14443-3.

As shown in FIG. 1, the IC card 1 has a main body C. The main body C is formed in a card shape by plastic or the like. The IC card 1 has a module M in the main body C. The module M is formed integrally with one or more IC chips Ca and an external interface (interface) for communication

which are connected to each other, and is embedded in the main body C.

Note that the portable electronic device according to the embodiment may include a module M in the main body C
5 that is formed in a booklet shape or may include a module M in the main body C that forms a portable electronic device.

In the configuration example shown in FIG. 1, the module M of the IC card 1 includes a processor 11, a RAM 12, a ROM 13, an NVM (memory) 14, a communication control
10 unit 15, an interface 16 and the like.

The processor 11 includes a circuit that performs a variety of processes. The processor 11 is, for example, a central processing unit (CPU). The processor 11 controls the entire IC card 1. The processor 11 executes programs
15 stored in the ROM 13 or the NVM 14 to implement a variety of processing functions. However, some or all of the functions executed by the processor 11 to be described later may be implemented by a hardware circuit.

The RAM 12 is a volatile memory that functions as a
20 working memory. The RAM 12 also functions as a buffer that temporarily stores data or the like which is being processed by the processor 11. For example, the RAM 12 functions as a communication buffer that temporarily stores data to be transmitted and received to and from the IC card
25 processing device 2 via the communication control unit 15 and the interface 16.

The ROM 13 is a nonvolatile memory that functions as a

program memory. The ROM 13 stores control programs and control data in advance. The ROM 13 is embedded into the IC card 1 with the control programs, control data and the like stored at the manufacturing stage. The control program and control data stored in the ROM 13 are integrated in advance in accordance with the specifications of the IC card 1.

For example, the ROM 13 stores a program for the processor 11 to execute a process corresponding to a command received from the IC card processing device 2. Since the IC card according to the embodiment is adapted to a plurality of cryptographic methods as a plurality of processing methods, the ROM 13 stores a program for performing a cryptographic process by its corresponding one of the cryptographic methods (new and existing cryptographic methods).

The NVM 14 is a nonvolatile memory capable of writing and rewriting data. The NVM 14 includes, for example, an electrically erasable programmable read only memory (EEPROM) (registered trademark), a flash ROM or the like. In addition, the NVM 14 includes a storage area part or all of which has tamper resistance and which is capable of storing data securely.

Programs and various items of data corresponding to the operation use of the IC card 1 are written into the NVM 14. Program files or data files are defined in the NVM 14, and programs and various items of data are written into the files. For example, the NVM 14 is provided with a storage

area that stores information indicating whether a cryptographic method is valid or invalid (information indicating validity) for some of the cryptographic methods. In addition, the NVM 14 may store cryptographic programs and cryptographic data such as key data for some of the cryptographic methods. The NVM 14 stores user data, network authentication data for communicating with an external network, application programs for executing a variety of processes, and the like.

10 The communication control unit 15 is connected to the interface 16. The interface 16 is an interface for communication connection to an external device. The communication control unit 15 and the interface 16 constitute a communication unit. The communication control unit 15 and the interface 16 fulfills a communication function according to a communication system corresponding to the interface of the IC card processing device 2. In addition, the communication control unit 15 and the interface 16 may be configured to support a plurality of communication systems (communication protocols) even in the case of contact communication or non-contact communication.

25 In the case where the IC card 1 is implemented as a contact IC card, the communication control unit 15 and the interface 16 constitute a communication unit which performs contact communication with the IC card processing device 2. In this case, the interface 16 includes a contact portion that is in physical and electrical contact with the contact

portion of the IC card processing device 2, and the communication control unit 15 includes a circuit or the like which controls transmission and reception of signals through the contact portion. In addition, the communication control unit 15 controls communication according to a communication system (communication protocol) designated by the processor 11.

In the case where the IC card 1 is implemented as a non-contact IC card, the communication control unit 15 and the interface 16 constitute a communication unit which performs non-contact (wireless) communication with a card reader/writer of the IC card processing device 2. In this case, the interface 16 includes an antenna that transmits and receives radio waves, and the communication control unit 15 includes, for example, a modulation circuit for generating radio waves to be transmitted and a demodulation circuit for generating signals from the received radio waves. In addition, the communication control unit 15 that performs non-contact communication controls communication according to a communication system (communication protocol) such as Type A and Type B designated by the processor 11.

FIG. 2 is a block diagram schematically showing a configuration example of the IC card processing device 2 according to the embodiment.

In the configuration example shown in FIG. 2, the IC card processing device 2 is a device (R/W) having a

function of communicating with the IC card 1 via a card reader/writer 24. The IC card processing device 2 may be, for example, a device in which the card reader/writer 24 is connected to a control device such as a personal computer (PC).

As shown in FIG. 2, the IC card processing device 2 includes a control unit 21, a display unit 22, an operation unit 23, a card reader/writer 24 and the like.

The control unit 21 controls the entire operation of the IC card processing device 2. The control unit 21 includes a processor (CPU) 25, a RAM 26, a ROM 27, a nonvolatile memory 28, a communication unit 29 and the like. For example, the control unit 21 includes a personal computer. The processor 25 executes various processes by executing programs stored in the ROM 27 or the nonvolatile memory 28. The RAM 26 functions as a working memory that temporarily holds data. The ROM 27 is a nonvolatile memory that stores programs, control data and the like. The nonvolatile memory 28 is a rewritable nonvolatile memory. The communication unit 29 is an interface for communicating with an external device.

The control unit 21 has a function of transmitting a command to the IC card 1 by the card reader/writer 24, a function of performing various processes based on data received from the IC card 1, and the like. For example, the control unit 21 transmits a data write command to the IC card 1 via the card reader/writer 24 to write data to the

nonvolatile memory in the IC card 1. The control unit 21 also transmits a read command to the IC card 1 to read data from the IC card 1. In addition, the control unit 21 transmits an application selection command to the IC card 1 to control an application selected by the IC card 1.

In the present embodiment, the control unit 21 of the IC card processing device 2 supplies the IC card 1 with information such as commands, which will be described later in each operation example, to designate a cryptographic method to be used by the IC card 1 for cryptographic processing.

The display unit 22 is a display device that displays various items of information under the control of the control unit 21. The operation part 23 includes a keyboard, a numeric keypad, a pointing device and the like. The operation unit 23 is designed to cause the operator of the IC card processing device 2 to input a variety of operation instructions, data and the like. The operation unit 23 also functions as an input unit for inputting identification information of the user of the IC card 1 or authentication information such as a password.

The card reader/writer 24 is a communication unit (second communication unit) for communicating with the IC card 1. The card reader/writer 24 includes an interface corresponding to the communication system of the IC card 1. In the case where the IC card 1 is a contact IC card, the card reader/writer 24 includes a contact portion that is in

physical and electrical contact with the contact portion of the IC card 1. In the case where the IC card 1 is a non-contact IC card, the card reader/writer 24 includes a communication controller and an antenna for performing radio communication with the IC card 1. The card reader/writer 24 supplies the IC card 1 with a power supply and a clock for operation. The card reader/writer 24 transmits a command to the IC card 1 and receives a response to the command from the IC card 1 under the control of the control unit 21.

Next is a description of the configuration of a file for storing data in the NVM 14 of the IC card 1 according to the embodiment.

The NVM 14 of the IC card 1 causes data to be stored in, for example, each of the files having a file structure defined by ISO/IEC 7816-4 that is an international standard for IC cards. In this file structure, a plurality of file groups having a hierarchical structure including a master file (MF), a dedicated file (DF), an elementary file (EF) and the like are defined.

The MF is at the top of the hierarchical structure, one or more DFs are defined at the level next to the MF, and one or more EFs are defined at the level next to the DF. One DF stores, for example, a data group for implementing one application provided in the IC card 1. In the IC card 1 that fulfills a plurality of functions by a plurality of applications, the NVM 14 includes a plurality

of DFs corresponding to their respective applications. Each of the EFs under the DF is a data file for storing various items of data to be used for applications as a DF of a higher level.

5 Next is a description of different processing methods for performing a specific process provided in the IC card 1 according to the embodiment.

10 The IC card 1 according to the embodiment is adapted to different processing methods (cryptographic methods) for performing a cryptographic process as a specific process. The IC card 1 has a function of performing a specific process by one selected from a plurality of processing methods. It is assumed in the present embodiment that the IC card 1 as a portable electronic device is adapted to an
15 existing cryptographic method (existing cryptographic method, first cryptographic) and a cryptographic method different from the existing cryptographic method (new cryptographic method, second cryptographic method). In addition, the IC card 1 according to the present embodiment
20 also has a function of performing a cryptographic process using either one selected from the existing cryptographic method and the new cryptographic method as a plurality of cryptographic methods.

25 It is assumed in the present embodiment that the new cryptographic method can execute a cryptographic process whose cryptographic strength is higher than the existing cryptographic method. For example, quantum-resistant

cryptography is assumed as a new cryptographic method. The quantum-resistant cryptography is a generic term for the cryptographic methods that are considered difficult to break even with a quantum computer. Examples of the quantum-resistant cryptography include lattice-based cryptography. Examples of the existing cryptographic method include RSA and data encryption standard (DES). The RSA is an algorithm for data cryptography using public key cryptography. The DES is an algorithm for data cryptography using common key cryptography. The cryptography methods of the quantum-resistant cryptography, RSA, DES and the like vary in, for example, the amount of computation required to perform a cryptographic process. In general, the quantum-resistant cryptograph has a higher cryptographic strength (higher security level) and a larger cryptography processing load (computation amount) than the RSA and DES.

FIG. 3 is a diagram schematically showing a storage area of the NVM 14 in the IC card 1 according to the embodiment, which stores setting information indicating a state (validity) for each of the cryptographic methods. FIG. 4 is a diagram schematically showing a storage area of the RAM 12 in the IC card 1 according to the embodiment, which stores setting information (cryptographic method identification flag) indicating a cryptographic method that is being selected (set).

As shown in FIG. 3, the NVM 14 of the IC card 1 has a storage area which stores information indicating whether

the existing cryptographic method is valid or invalid and information indicating whether the new cryptographic method is valid or invalid. For example, if the existing cryptographic method and the new cryptographic method are both valid, the NVM 14 stores information indicating that the existing cryptographic method is valid and information indicating that the new cryptographic method is valid as setting information (flag) of the cryptographic methods. If the existing cryptographic method is set to be invalid while the new cryptographic method remains valid, the NVM 14 stores setting information indicating that the existing cryptographic method is invalid and the new cryptographic method is valid.

The RAM 12 of the IC card 1 stores information indicating a cryptographic method that is being selected as a cryptographic method identification flag. According to the example shown in FIG. 4, the IC card 1 indicates that a new cryptographic method (a cryptographic process in the new cryptographic method) is selected as a cryptographic method when the cryptographic method identification flag is in a state ("11") indicating the new cryptographic method, and indicates that a new cryptographic method (a cryptographic process in the new cryptographic method) is selected as a cryptographic method when the cryptographic method identification flag is in a state ("22") indicating the existing cryptographic method.

Note that since one of the existing and new

cryptographic methods need not be invalidated if there is no time limit for the coexistence of the cryptographic methods, there may be no setting for invalidating one of the cryptographic methods as described above. For example,
5 if the IC card 1 is issued as a credit card or the like, it need not be set to invalidate any cryptographic method unless there is an operating plan to invalidate any cryptographic method by the expiration date of the operation.

10 Next is a description of an operation example (first to third operation examples) including a process in which the IC card 1 as a portable electronic device according to the embodiment selects a cryptographic method in response to a command from the IC card processing device 2.

15 First is a description of a first operation example of the IC card 1 as a portable electronic device according to the embodiment.

FIG. 5 is a flowchart illustrating a flow of the first operation example of the IC card 1 as a portable electronic
20 device according to the embodiment.

The IC card 1 is connected to the IC card processing device 2 via the interface 16 by means of the communication control unit 15. When the IC card 1 is connected to the IC card processing device 2, the processor 11 of the IC card 1
25 is started by power applied from the IC card processing device 2.

The processor 11 of the IC card 1 performs a reset in

response to a reset request (command) from the IC card processing device 2. The processor 11 of the IC card 1 determines a type of the reset to be performed in response to the request from the IC card processing device 2 (step
5 ST11). In the example shown in FIG. 5, the processor 11 determines whether the reset is a cold (COLD) reset or a warm (WARM) reset.

The cold reset is an operation of starting (resetting) various memories and programs as initial states. The warm
10 reset is an operation of starting (resetting) information and programs held in the memories without being set in initial states. For example, the cold reset is performed immediately after the power supply is turned on, and the warm reset is a start operation performed while maintaining
15 the information held in the memories and the state of the programs when the power supply is in an ON state. For example, the cold reset and warm reset in the IC card 1 may be defined in ISO/IEC7816-3.

Upon request of a cold reset from the IC card
20 processing device 2 (Yes in step ST11), the processor 11 performs the cold reset (step ST12). In the cold reset, the processor 11 sets a new cryptographic method as a cryptographic method to be used for cryptographic processing (step ST13). For example, the processor 11 sets
25 data indicating a new cryptographic method as a cryptographic method identification flag to be stored in the RAM 12. Completing the cold reset, the processor 11

transmits a response indicating that the cold reset is completed (ATR: Answer To Reset) to the IC card processing device 2 (step ST14).

5 Upon request of a warm reset from the IC card processing device 2 (No in step ST11), the processor 11 performs the warm reset (step ST15). The timing for requesting the warm reset is requested by the IC card processing device 2 in accordance with the process for the IC card 1. In the warm reset operation, the processor 11
10 sets an existing cryptographic method as a cryptographic method to be used for cryptographic processing (step ST16). For example, the processor 11 sets data indicating an existing cryptographic method as a cryptographic method identification flag to be stored in the RAM 12. Completing
15 the warm reset, the processor 11 transmits a response (ATR) indicating that the warm reset is completed to the IC card processing device 2 (step ST17).

20 When the processor 11 of the IC card 1 performs the reset operation, it receives various commands from the IC card processing device 2 (step ST18).

 When the processor 11 receives the commands, it performs a process (command process) in response to the commands (step ST19). The command process will be described in detail later. The processor 11 transmits a response
25 indicating the result of the command process (step ST20), and returns to step ST18 to enter a command waiting state.

 As described above, in the IC card according to the

first operation example, a cryptographic method is selected in accordance with the type of a reset requested from the IC card processing device and set in the reset operation. For example, the IC card sets the new cryptographic method as a second cryptographic method in the cold reset operation when a cold reset is requested from the IC card processing device, and sets the existing cryptographic method as a first cryptographic method in the warm reset operation when a warm reset is requested from the IC card processing device.

Note that the foregoing second cryptographic method and first cryptographic method may be reversed from the example described above. That is, the IC card may set the existing cryptographic method as a second cryptographic method in the cold reset operation when a cold reset is requested from the IC card processing device, and set the new cryptographic method as a first cryptographic method in the warm reset operation when a warm reset is requested from the IC card processing device.

According to the first operation example as described above, the IC card can set a cryptographic method in accordance with the type of a reset requested from the IC card processing device. Correspondingly, the IC card processing device can specify a cryptographic method according to the type of a reset required for the IC card.

As a specific example, the IC card can set the new cryptographic method when performing a cold reset operation

in response to a cold reset request from the IC card processing device, and set the existing cryptographic method when performing a warm reset operation in response to a warm reset request from the IC card processing device.

5 In other words, the IC card processing device can set a new cryptographic method having a strong cryptographic strength such as quantum-resistant cryptography to the IC card in a cold reset in which various items of information are brought into default states, and can set an existing

10 cryptographic method to the IC card in a warm reset in which various items of information are held.

Next is a description of a second operation example of the IC card 1 as a portable electronic device according to the embodiment.

15 FIG. 6 is a flowchart illustrating a flow of the second operation example of the IC card 1 as a portable electronic device according to the embodiment.

The IC card 1 is connected to the IC card processing device 2 via the interface 16 by means of the communication control unit 15, and is started by power applied from the

20 IC card processing device 2. The processor 11 of the IC card 1 performs a reset in response to a reset request from the IC card processing device 2 (step ST31).

Upon completing the reset operation, the processor 11

25 transmits a reset response (ATR) to the IC card processing device 2 (step ST32). For example, upon request of a cold reset from the IC card processing device 2, the processor

11 performs the cold reset and transmits an ATR
corresponding to the cold reset. Upon request of a warm
reset from the IC card processing device 2, the processor
performs the warm reset and transmits an ATR corresponding
5 to the warm reset.

Upon transmitting an ATR, the processor 11 sets a
communication condition including a communication rate
(communication speed) corresponding to the ATR to be
transmitted to the IC card processing device 2 (step ST33),
10 and sets an existing cryptographic method as a default
cryptographic method of the IC card 1 (step ST34). Upon
setting the communication condition and the cryptographic
method, the processor 11 receives various commands from the
IC card processing device 2.

15 Upon receiving a request to set (change) a
communication condition such as a communication rate as a
command from the IC card processing device 2 (Yes in step
ST35), the processor 11 changes the communication condition
in response to the command (step ST36). For example,
20 according to ISO/IEC7816-3 that is a standard for the
contact IC card, the IC card processing device 2 requests
the IC card 1 to set a communication rate by a command
called PPS request. In response thereto, the IC card 1
changes the communication rate to that requested by the PPS
25 request and returns a PPS response to the IC card
processing device 2. If the IC card 1 is a non-contact IC
card, the communication rate can be changed by PPS request

and PPS response specified in ISO/IEC14443-4.

When a communication condition is changed, the processor 11 of the IC card 1 determines whether or not it is changed to a communication condition for which a new cryptographic method is set (step ST37). For example, setting information indicating communication conditions such as a communication rate at which a new cryptographic method should be set is stored in the NVM 14 or the like. The processor 11 determines, based on the setting information stored in the NVM 14, whether a communication condition such as a communication rate is that for which a new cryptographic method should be set.

When the communication condition is changed to that for which a new cryptographic method should be set (Yes in step ST37), the processor 11 sets the cryptographic method for use in cryptographic processing to the new cryptographic method (step ST38). If the communication condition is not that for which the new cryptographic method should be set (No in step ST37), the processor 11 keeps the cryptographic method for use in cryptographic processing as the existing cryptographic method.

In addition, upon receiving a command other than the communication rate setting request from the IC card processing device 2 (step ST39), the processor 11 of the IC card 1 executes a process (command process) corresponding to the received command (step ST40). Upon executing the command process, the processor 11 transmits a response as a

result of the command process (step ST41), and returns to step ST35 to enter the command waiting state.

As described above, the IC card according to the second operation example sets the existing cryptographic method (first processing method) of default setting in the
5 reset operation. If the communication condition changed in response to a request (command) from the IC card processing device is a communication condition for setting the new cryptographic method (second processing method), the IC
10 card changes the cryptographic method for use in the cryptographic processing is changed to the new cryptographic method.

According to the second operation example described above, the IC card can set the cryptographic method
15 according to the communication setting requested from the IC card processing device and can switch the cryptographic method according to the change of the communication setting from the IC card processing device. In response thereto, the IC card processing device can specify the cryptographic
20 method of the IC card in accordance with a communication condition (communication rate) required for the IC card with optional timing.

As a specific example, when the communication rate of the IC card is increased in response to a request from the
25 IC card processing device, the cryptographic method for use in cryptographic processing can be switched to the new cryptographic method in the command process. Since the new

cryptographic method is expected to increase the amount of data required for cryptography, its convenience is improved if it is implemented at high speed. If, furthermore, the existing cryptographic method is set in a default state for the IC card, the existing system that performs a process using the existing cryptographic method can be used as it is.

Next is a description of a third operation example of the IC card 1 as the portable electronic device according to the embodiment.

FIG. 7 is a flowchart illustrating a flow of the third operation example of the IC card 1 as the portable electronic device according to the embodiment.

Assume here that the IC card 1 according to the third operation example shown in FIG. 7 is adapted to a plurality of communication systems (communication protocols) and has a function of selecting one of the communication systems in response to a request from the IC card processing device 2. For example, the non-contact IC card specified in ISO/IEC14443-3 has "Type A," "Type B" and the like as communication systems. The IC card processing device 2 supports at least one communication system to communicate with an IC card to be processed.

Upon receiving a request for a communication system (communication protocol) from the IC card processing device 2 (Yes in step ST51), the processor 11 of the IC card 1 transmits a response indicating a supportable communication

condition in response to the request from the IC card processing device 2 (step ST52). For example, in the case of "Type B," the IC card processing device 2 transmits a command of REQB (REQuest command, Type B) to the IC card 1.

5 In response thereto, the processor 11 of the IC card 1 returns a response of ATQB (Answer to Request, Type B). Here, the response of the ATQB indicates a plurality of communication speeds that can be supported between the IC card processing device 2 and the IC card 1, and
10 communication conditions such as a buffer size of communication data.

Upon receiving a command for specifying a communication condition from the IC card processing device 2, the processor 11 of the IC card 1 makes communication
15 setting under the specified communication condition (step ST53). For example, the IC card processing device 2 selects a parameter (communication speed, buffer size, etc.) as a communication condition from a plurality of communication speeds indicated by the above-described ATQB from the IC
20 card 1, and transmits an ATTRIB (PICC selection command, Type B) command that specifies the selected communication condition to the IC card. The processor 11 of the IC card 1 sets the communication condition specified by the ATTRIB from the IC card processing device 2 and responds with an
25 Answer to ATTRIB command. Accordingly, the IC card 1 performs communication by the parameter (communication speed, buffer size, etc.) specified by the IC card

processing device 2.

When the processor 11 of the IC card 1 sets the communication condition specified by the IC card processing device 2, it selects a cryptographic method corresponding to the set communication system and communication condition (step ST54). For example, the processor 11 of the IC card 1 selects either the existing cryptographic method or a new cryptographic method in accordance with a parameter (e.g., communication speed, buffer size, etc.) specified by the ATTRIB command.

For example, the processor 11 of the IC card 1 selects a cryptographic method as a communication condition based on setting information for each of the communication systems stored in a memory such as the NVM 14. As a specific example, in Type B, setting information is stored in the NVM 14 such that if the communication speed is 106 kbps, the existing cryptographic method is set, and if the communication speed is not 106 kbps, a new cryptographic method is set. The IC card 1 in which such setting information is stored sets the existing cryptographic method if the communication speed specified in the ATTRIB is 106 kbps, and sets a new cryptographic method if it is not 106 kbps.

That is, when the processor 11 selects a new cryptographic method in accordance with the communication system and the communication condition (Yes in step ST54), it sets the new cryptographic method as a cryptographic

method for performing a cryptographic process (step ST55).
In addition, when the processor 11 selects an existing
cryptographic method in accordance with the communication
system and the communication condition (No in step ST54),
5 it sets the existing cryptographic method as a
cryptographic method for performing a cryptographic process
(step ST56).

Upon receiving a command other than a communication
system request from the IC card processing device 2 (Yes in
10 step ST57), the processor 11 of the IC card 1 performs a
process (command process) in response to the received
command (step ST58). When the processor 11 performs the
command process, it transmits a response indicating a
result of the command process (step ST59), and returns to
15 step ST51 to enter a state of waiting for receiving a
communication setting request or other commands.

As described above, the IC card according to the third
operation example holds setting information indicating a
communication condition for selecting a cryptographic
20 method for each communication system (communication
protocol), and sets a processing method (cryptographic
method) based on the setting information for each
communication system when the communication system is set
(selected). The IC card processing device specifies a
25 processing system to be set in the IC card under the
communication condition in the specified communication
system of the IC card.

According to the third operation example described above, the IC card can set a processing method for performing a specific process in accordance with a communication condition for each communication system requested from the IC card processing device, and select a processing method according to the information set for each communication system. The IC card processing device can also specify a processing method of the IC card according to the communication condition for each communication system.

Next is a description of an operation example (fourth operation example) including a process in which the IC card 1 as the portable electronic device according to the embodiment notifies the IC card processing device 2 of a cryptographic method corresponding to the IC card 1 itself.

FIG. 8 is a flowchart illustrating a flow of the fourth operation example of the IC card 1 as the portable electronic device according to the embodiment.

The fourth operation example is an example of an operation including a process of notifying the IC card processing device 2 of a cryptographic method (executable cryptographic method) in which the IC card 1 is valid.

In the example shown in FIG. 8, first, it is assumed that the processor 11 of the IC card 1 receives a reset (cold reset) request immediately after power is applied from the IC card processing device 2. Upon request for a cold reset from the IC card processing device 2 (Yes in

step ST61), the processor 11 executes the cold reset (step ST62). The processor 11 sets a new cryptographic method as a cryptographic method to be used for cryptographic processing in the cold reset (step ST63). Upon completion
5 of the cold reset, the processor 11 transmits a response (ATR) indicating the completion of the cold reset to the IC card processing device 2 (step ST64).

After performing the reset operation, the processor 11 of the IC card 1 receives a variety of commands from the IC
10 card processing device 2 (step ST69). Upon receiving a command other than the reset request from the IC card processing device 2 (Yes in step ST70), the processor 11 performs a process (command process) in response to the received command (step ST71).

15 When the processor 11 performs the command process, it determines whether the existing cryptographic method (which is a cryptographic method other than the new cryptographic method set by default (cold reset)) is valid (step ST72). For example, the processor 11 determines whether the
20 existing cryptographic method is valid or invalid based on information indicating a cryptographic method setting flag stored in the NVM 14.

If the existing cryptographic method is valid (Yes in step ST72), the processor 11 sets information indicating
25 that the existing cryptographic method is valid in response data indicating a result of the command process (step ST73). The processor 11 transmits to the IC card processing

device 2 the response data in which data indicating that the existing cryptographic method is valid is set (step ST75), and returns to step ST69 to enter a command waiting state. Note that the information indicating that the existing cryptographic method is valid may include information indicating that the existing cryptographic method is valid in a status word indicating the result of the command process, or data indicating that the existing cryptographic method is valid may be set in the response data.

If the existing cryptographic method is not valid (No in step ST72), the processor 11 sets data indicating that the existing cryptographic method is invalid in response data indicating a result of the command process (step ST74). The processor 11 transmits to the IC card processing device 2 the response data in which data indicating that the existing cryptographic method is invalid is set (step ST75), and returns to step ST69 to enter a command waiting state.

If, however, the existing cryptographic method is valid and the result of the command process is abnormal as the process of steps ST73 to ST75, the processor 11 may transmit response data indicating normal abnormality, and if the existing cryptographic method is valid and the result of the command process is normal, it may transmit response data indicating that the result of the process is normal and the existing cryptographic method is valid.

In the fourth operation example described above, the validity of a cryptographic method is notified in response to a command in the operation of setting the cryptographic method in accordance with the type of reset as described in the first operation example. In the operation example shown in FIG. 8, the operation described in the second operation example or the third operation example may be applied to the operation of selecting a cryptographic method to be set. That is, the operation of setting a cryptographic method in accordance with the reset type may be replaced with an operation of setting a cryptographic method in accordance with the communication condition such as a communication rate.

In the fourth operation example described above, it is based on the premise that in the IC card 1, the cryptographic method set in the cold reset (default state) is a new cryptographic method. Thus, in the process of steps ST72 to ST74 (the process of response to the command), the IC card 1 transmits to the IC card processing device 2 a command response including information indicating whether the existing cryptographic method, which is a cryptographic method other than the new cryptographic method set in the default state (cold reset), is valid.

The fourth operation example is also applicable to the case where the existing cryptographic method is set in the default state of the IC card 1 as a modification. That is, if the existing cryptographic method is set in the default

state of the IC card 1, the IC card 1 may transmit to the IC card processing device 2 a command response including information indicating whether the new cryptographic method, which is a cryptographic method other than the existing cryptographic method set in the default state, is valid in the process of response to the command in step ST72 to ST74.

As another modification, in the fourth operation example, a response indicating information representing the validity of each of the cryptographic methods (new cryptographic method and existing cryptographic method) corresponding to the IC card 1 in the response indicating a result of the command process, regardless of the cryptographic method set by the IC card 1 in the default state. That is, in the fourth operation example, the process of steps ST72 to ST74 may be replaced with a process of outputting a response indicating information representing the validity of each of the cryptographic methods (new cryptographic method and existing cryptographic method).

As described above, the IC card according to the fourth operation example outputs a response including information indicating the validity of each cryptographic method in the IC card when it performs a command process in response to a command from the IC card processing device. According to the fourth operation example, in response to the command process, the IC card can transmit to the IC

card processing device information indicating a cryptographic method that can be executed by the IC card.

5 The IC card according to the fourth operation example described above outputs a response indicating a result of the command process including information indicating whether a cryptographic method other than the cryptographic method set in the default state is valid. According to the fourth operation example, the IC card can transmit to the IC card processing device information indicating whether a
10 cryptographic method other than the cryptographic method set in the default state is valid in response to the command process.

Next is a description of an operation example (fifth operation example) of a process in which the IC card 1 as
15 the portable electronic device according to the embodiment invalidates a specific cryptographic method as a command process.

FIG. 9 is a flowchart illustrating a flow of the fifth operation example of the IC card 1 as the portable
20 electronic device according to the embodiment.

FIG. 9 is a flowchart illustrating, as the fifth operation example, an example of a process for invalidating a specific cryptographic method, which is performed as one of the command processes in FIGS. 5 to 8. In the fifth
25 operation example, the IC card 1 performs a process of invalidating a specific cryptographic method designated by the IC card processing device 2 among a plurality of

corresponding cryptographic methods.

Upon receiving a command from the IC card processing device 2 in the above-described processes shown in FIGS. 5 to 8, the processor 11 of the IC card 1 performs a command process.

Upon receiving a command from the IC card processing device 2, the processor 11 determines whether or not the received command is a command for requesting invalidation of the cryptographic method (step ST81). For example, if the received command has a format as shown in FIG. 11, which will be described later, the processor 11 determines whether or not the received command requests invalidation of the cryptographic method according to whether or not data indicating that invalidation of the cryptographic method is requested is set in "CLA/INS," which is identification information of the command. As a specific example, the IC card processing device 2 transmits to the IC card 1 a command for requesting invalidation of the existing cryptographic method when the existing cryptographic method of the IC card 1 is invalidated. Accordingly, the processor 11 of the IC card 1 receives the command for requesting invalidation of the existing cryptographic method.

Upon receiving a command for requesting invalidation of a specific cryptographic method (Yes in step ST81), the processor 11 performs a process of invalidating a cryptographic method specified by the received command

(step ST82). For example, the processor 11 stores in the NVM 14 information indicating the invalidation of the cryptographic method specified by the command to invalidate the specified cryptographic method. As a specific example, upon receiving a command for requesting invalidation of the existing cryptographic method, the processor 11 of the IC card 1 updates the cryptographic method setting flag in the NVM 14 as shown in FIG. 3 to information indicating invalidation of the existing cryptographic method thereby to invalidate the existing cryptographic method.

When the processor 11 invalidates the cryptographic method specified by the command, it generates response data including information indicating that the specified cryptographic method is invalidated as data indicating a result of the command process (step ST84). When the processor 11 generates the response data, it transmits to the IC card processing device 2 the response data indicating the result of the command process as shown in FIGS. 5 to 8. Accordingly, the IC card processing device 2, which is the transmission source of the command, confirms that the specified cryptographic method is invalidated in the IC card 1.

Upon receiving a command other than the command for requesting invalidation of the cryptographic method (No in step ST81), the processor 11 performs a processing (command process) corresponding to the received command (step ST83) and generates response data indicating a result of the

command process (step ST84).

As described above, the IC card according to the fifth operation example invalidates the specified cryptographic method in response to a command requested from the IC card processing device. Thus, an IC card, which is adaptable to a plurality of cryptographic methods, can invalidate a specific cryptographic method in response to a command from the IC card processing device. As a result, even after an IC card capable of executing a plurality of cryptographic methods is issued and processed, a specific one of the cryptographic methods in which vulnerability is found can be invalidated in response to a command from the IC card processing device.

For example, upon receiving a command requesting invalidation of the existing cryptographic method from the IC card processing device, the IC card according to the fifth operation example invalidates the existing cryptographic method in response to the received command. Thus, even if an IC card capable of executing the existing cryptographic method and the new cryptographic method is issued during the transition period from the existing cryptographic method to the new cryptographic method, the existing cryptographic method can be invalidated after the transition period. As a result, the cryptographic method can be invalidated by the existing cryptographic method with weak cryptographic strength after the transition period, and the operation in the transition period during

which the existing cryptographic method and the new cryptographic method coexist can be smoothly performed, as can be the operation after the transition period.

According to the fifth operation example described
5 above, the IC card adaptable to the new cryptographic method and the existing cryptographic method can invalidate the existing cryptographic method having a weaker cryptographic strength than the new cryptographic method in response to a command from the IC card processing device.
10 As a result, the IC card can be operated in such a manner that a cryptographic process is performed using any cryptographic method selected from the existing cryptographic method and the new cryptographic method during a transition period in which the entire system
15 including the IC card and the IC card processing device is shifted from the existing cryptographic method to the new cryptographic method, and the existing cryptographic method having a weak cryptographic strength is invalidated after the transition period.

20 Next is a description of an operation example (sixth operation example) including a process in the case where the IC card 1 as the portable electronic device according to the embodiment receives a signature verification command, which is an example of the command process
25 requesting a process including a cryptographic process.

FIG. 10 is a flowchart illustrating a flow of the sixth operation example of the IC card 1 as the portable

electronic device according to the embodiment.

In the sixth operation example, the IC card 1 sets one of a plurality of cryptographic methods. Upon receiving a command for a process including a cryptographic process, the IC card 1 performs a process including the cryptographic process using the set cryptographic method. In other words, in the sixth operation example, it is assumed that the command for a process including a cryptographic process (signature verification command) has the same contents (a command in which the same data or data equivalent to the same data is set) regardless of which cryptographic method is set.

In the operation example shown in FIG. 10, the processor 11 of the IC card 1 performs a reset operation in response to a reset request from the IC card processing device 2 (step ST90). Upon completion of the reset operation, the processor 11 transmits a reset response (ATR) to the IC card processing device 2 (step ST91). In addition, when the processor 22 transmits the ATR, it sets a communication condition including a communication rate that is adapted to the ATR to be transmitted to the IC card processing device 2 (step ST92). When the processor 11 sets the communication condition, it accepts various commands from the IC card processing device 2 (step ST93).

Upon receiving a command (Yes in step ST93), the processor 11 of the IC card 1 determines whether or not the received command is a command that requires a process

including the cryptographic process (step ST94). An example of the command that requires a process including the cryptographic process is a signature verification command. Assume here that a command that requires a process including the cryptographic process is a signature verification command as shown in FIG. 10.

FIG. 11 is a diagram showing a configuration example of a format of a signature verification command that is an example of the command that requires a process including the cryptographic process.

The format of the command as shown in FIG. 11 includes "CLA/INS" as command identification information and "P1P2" as a parameter. FIG. 11 shows an example of the signature verification command, in which "0088" is set in the "CLA/INS." That is, a command whose format has "CLA/INS" of "0088" represents a signature verification command. In the sixth operation example, a signature verification command as shown in FIG. 11 is used without depending on the cryptographic method. In other words, in the sixth operation example, the signature verification command is a common command for the existing cryptographic method and the new cryptographic method as shown in FIG. 11.

If the received command is a command that requests a process including the cryptographic process (signature verification command) (Yes in step ST94), the processor 11 determines whether the cryptographic method selected by the IC card 1 under the communication condition is a new

cryptographic method or an existing cryptographic method
(step ST95). If the cryptographic method to be selected
under the communication condition is a new cryptographic
method (Yes in step ST95), the processor 11 performs a
5 signature verification process as a process including the
cryptographic process using a new cryptographic method in
response to the signature verification command (step ST96).
When the processor 11 performs signature verification
including the cryptographic process using a new
10 cryptographic method, it transmits response data indicating
a processing result of the signature verification to the IC
card processing device 2 (step ST99).

If the cryptographic method set in the IC card 1 is an
existing cryptographic method (No in step ST95), the
15 processor 11 performs a signature verification process as a
process including the cryptographic process using the
existing cryptographic method in response to the signature
verification command (step ST98). When the processor 11
performs signature verification including the cryptographic
20 process using the existing cryptographic method, it
transmits response data indicating a processing result of
the signature verification to the IC card processing device
2 (step ST99).

Upon receiving a command other than a command that
25 requests a process including the cryptographic process
(signature verification command) (No in step ST94), the
processor 11 performs a process in response to the received

command (step ST97) and transmits response data indicating a result of the command process to the IC card processing device 2 (step ST99).

As described above, the IC card according to the sixth operation example performs a cryptographic process using the cryptographic method set (selected) in the IC card. Thus, the IC card need not specify (identify) a cryptographic method to be used for cryptographic processing from a command that requests a process including the cryptographic processing, and the IC card processing device need not change data of the command to designate the cryptographic method to be used for the cryptographic processing. For example, if the IC card according to the sixth operation example is executed in combination with the first operation example, it has only to set a cryptographic method in the reset operation, and it need not specify a cryptographic method in the command that requests the cryptographic processing.

Next is a description of an operation example (seventh operation example) in the case where the IC card 1 as the portable electronic device according to the embodiment receives a signature verification command that is an example of a command that requests a process including a cryptographic process.

FIG. 12 is a flowchart illustrating a flow of the seventh operation example of the IC card 1 as the portable electronic device according to the embodiment.

In the seventh operation example, the IC card 1 performs a cryptographic process using a cryptographic method specified by a parameter in the command of a process including a cryptographic process (for example, a signature verification command). In other words, the IC card of the seventh operation example specifies which cryptographic method is to be used for the cryptographic process by a parameter in the command of a process including a cryptographic process.

10 In the operation example shown in FIG. 12, first, the processor 11 of the IC card 1 performs a reset operation in response to a reset request from the IC card processing device 2 (step ST100). Upon completion of the reset operation, the processor 11 transmits a reset response (ATR) to the IC card processing device 2 (step ST101). When transmitting the ATR, the processor 11 sets a communication condition including, for example, a communication rate corresponding to the ATR to be transmitted to the IC card processing device 2 (step ST102). Upon setting the communication condition, the processor 11 accepts a variety of commands from the IC card processing device 2 (step ST103).

25 Upon receiving a command from the IC card processing device 2 (Yes in step ST103), the processor 11 of the IC card 1 determines whether or not the received command is a command (signature verification command) that requests a process including a cryptographic process (step ST104).

Upon receiving a command other than the signature verification command (No in step ST104), the processor 11 performs a command process corresponding to the received command (step ST105), and transmits response data
5 indicating a result of the command process to the IC card processing device 2 (step ST111).

If the received command is a signature verification command (Yes in step ST104), the processor 11 determines whether the data set in the parameter of the signature
10 verification command specifies a new cryptographic method or an existing cryptographic method. That is, the processor 11 specifies a cryptographic method to be used for the cryptographic process of signature verification based on the parameter of the received signature verification
15 command.

FIG. 13 is a diagram showing an example in which data that specifies an existing cryptographic method is set in parameters of signature verification commands. FIG. 14 is a diagram showing an example in which data that specifies a
20 new cryptographic method is set in parameters of signature verification commands.

In the example of the signature verification commands shown in each of FIGS. 13 and 14, "P1" and "P2" as parameters are defined as follows.

25 Parameter "P2" specifies a cryptographic method. For example, if "P2" is "01," it specifies an existing cryptographic method. If "P2" is "02," it specifies a new

cryptographic method. In addition, "P1" indicates an identifier of a key for use in signature data. In this case, if "P1" is "01," it indicates that key data of ID "01" is used. If "P1" is "02," it indicates that key data of ID "02" is used. Note that the key data is stored together with an identifier in a memory such as the NVM in the IC card 1.

As a specific example, in the example shown in FIG. 13, data set in parameters "P1" and "P2" of the signature verification commands are "01" and "01" and thus the cryptographic method is an existing cryptographic method and the ID of key data is "01." In the example shown in FIG. 14, data set in parameters "P1" and "P2" of the signature verification commands are "03" and "02" and thus the cryptographic method is a new cryptographic method and the ID of key data is "03."

If the parameter of a signature verification command is a new cryptographic method (Yes in step ST106), the processor 11 performs a signature verification process as a process including a cryptographic process using the new cryptographic method in response to the signature verification command (step ST107). When performing the signature verification process including a cryptographic process using the new cryptographic method, the processor 11 transmits response data indicating a result of the signature verification process to the IC card processing device 2 (step ST111).

If the parameter of a signature verification command is not a new cryptographic method (No in step ST106), the processor 11 determines whether or not the parameter of the signature verification command is an existing cryptographic method (step ST108). If the parameter of the signature verification command is an existing cryptographic method (Yes in step ST108), the processor 11 performs a signature verification process as a process including a cryptographic process using an existing cryptographic method in response to the signature verification command (step ST109). When performing the signature verification process including a cryptographic process using the existing cryptographic method, the processor 11 transmits response data indicating a result of the signature verification process to the IC card processing device 2 (step ST111).

If the parameter of a signature verification command is neither a new cryptographic method nor an existing cryptographic method (No in step ST108), the processor 11 determines that the parameter of the signature verification command is an error (abnormal value) (step ST110). When the parameter of the received signature verification command is an error, the processor 11 transmits to the IC card processing device 2 response data indicating that the parameter of the signature verification command is abnormal (step ST111).

As described above, the IC card according to the seventh operation example specifies a cryptographic method

according to the parameter of the received signature verification command and performs a signature verification process including a cryptographic process using a cryptographic method specified by the parameter. Thus, the IC card can specify a cryptographic method for use in the cryptographic process using the parameter of a command that requests a process including a cryptographic process. The IC card processing device can specify a cryptographic method to be used for the cryptographic process using a parameter of a command each time it request a process including the cryptographic process.

Next is a description of an operation example (eighth operation example) including a process in the case where the IC card 1 as the portable electronic device according to the embodiment receives a signature verification command that is an example of a command process that requests a process including a cryptographic process.

FIG. 15 is a flowchart illustrating a flow of the eighth operation example of the IC card 1 as the portable electronic device according to the embodiment.

The eighth operation example is an operation example in which identification information (CLA/INS) of the signature verification command is defined for each cryptographic method. The IC card 1 determines whether it is a signature verification command in the existing cryptographic system or a signature verification command in the new cryptographic system according to the

identification information of a command received from the IC card processing device 2. In other words, in the IC card of the eighth operation example, a signature verification command is defined for each cryptographic method; thus, a
5 cryptographic method to be used for cryptographic processing is specified by the identification information of the signature verification command.

For example, FIG. 16 is a diagram showing an example of a signature verification command that specifies an
10 existing cryptographic method. FIG. 17 is a diagram showing an example of a signature verification command that specifies a new cryptographic method.

The signature verification commands shown in FIGS. 16 and 17 are different in data (value) of "CLA/INS" that is
15 identification information of the commands. In the command shown in FIG. 16, "CLA/INS" is "008A." As shown in FIG. 16, the command whose "CLA/INS" is "008A" is defined as a signature verification command according to the existing cryptographic method. In the command shown in FIG. 17,
20 "CLA/INS" is "008 C." As shown in FIG. 17, the command whose "CLA/INS" is "008 C" is defined as a signature verification command according to the new cryptographic method.

In the operation example shown in FIG. 15, the
25 processor 11 of the IC card 1 performs a reset operation in response to a reset request from the IC card processing device 2 (step ST120). Upon completion of the reset

operation, the processor 11 transmits a reset response (ATR) to the IC card processing device 2 (step ST121). When transmitting the ATR, the processor 11 sets a communication condition including a communication rate corresponding to the ATR to be transmitted to the IC card processing device 2 (step ST102). Upon setting the communication condition, the processor 11 accepts a variety of commands from the IC card processing device 2 (step ST123).

Upon receiving a command from the IC card processing device 2, the processor 11 of the IC card 1 determines whether or not the received command is a command (signature verification command) which requires signature verification including a cryptographic process using a new cryptographic method (step ST124). According to the foregoing example shown in FIG. 16, the processor 11 determines whether or not the received command is a signature verification command that specifies a new cryptographic method according to whether or not the "CLA/INS" of the received command is "008C."

If the received command is a signature verification command that specifies a new cryptographic method (Yes in step ST124), the processor 11 performs a signature verification process including a cryptographic process using the new cryptographic method in response to the command (step ST125). When the processor 11 performs the signature verification process including a cryptographic process using the new cryptographic method, it transmits

response data indicating a result of the signature verification process to the IC card processing device 2 (step ST129).

5 If the received command is not a signature verification command that specifies a new cryptographic method (No in step ST124), the processor 11 determines whether or not the command is a signature verification command that specifies an existing cryptographic method (step ST126). If the received command is a signature
10 verification command that specifies an existing cryptographic method (Yes in step ST126), the processor 11 performs a signature verification process including a cryptographic process using the existing cryptographic method in response to the command (step ST127). When
15 performing the signature verification process including a cryptographic processing using the existing cryptographic method, the processor 11 transmits response data indicating a result of the signature verification process to the IC card processing device 2 (step ST129).

20 If the received command is not a signature verification command that specifies an existing cryptographic method, that is, if the received command is not a signature verification command (No in step ST126), the processor 11 performs a command process corresponding
25 to the received command (step ST128), and transmits response data indicating a result of the command process to the IC card processing device 2 (step ST129).

As described above, the IC card according to the eighth operation example identifies which cryptographic method is used for the signature verification command according to the identification information of the received command, and performs a signature verification process including a cryptographic process using the specified cryptographic method. As a specific example, the IC card performs a signature verification process including a cryptographic process using an existing cryptographic method upon receipt of a signature verification command that specifies the existing cryptographic method, and performs a signature verification process including a cryptographic process using a new cryptographic method upon receipt of a signature verification command that specifies the new cryptographic method.

Thus, the IC card can specify a cryptographic method for use in cryptographic processing using a command defined for each cryptographic method, and can perform a process including a cryptographic process using the specified cryptographic method. In addition, the IC card processing device can select a command for specifying a desired cryptographic method from among a plurality of types of commands defined for each cryptographic method to specify a cryptographic method to be used for cryptographic processing.

Note that the foregoing operation examples can be combined as appropriate. For example, the first to third

operation examples can be combined with the fourth to eighth operation examples, and the sixth to eighth operation examples can be combined with the first to fifth operation examples. In addition, the fourth and fifth operation examples can be further combined with the combinations of the other operation examples.

In addition, the functions described in the foregoing embodiment are not limited to a hardware configuration, but may be implemented by using software to cause a computer to read programs describing the functions. The functions may be configured by appropriately selecting either software or hardware.

While certain embodiments have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions. Indeed, the novel methods and systems described herein may be embodied in a variety of other forms; furthermore, various omissions, substitutions and changes in the form of the methods and systems described herein may be made without departing from the spirit of the inventions. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the inventions.

CLAIMS

1. A portable electronic device comprising:
an interface which communicates with an external
5 device;

a memory which stores setting information for each of
a plurality of different processing methods to perform a
specific process; and

a processor which selects one of the processing
10 methods to perform the specific process in accordance with
information supplied from the external device, and performs
the specific process by the selected one of the processing
methods.

2. The portable electronic device of claim 1, wherein:
15 the specific process is a cryptographic process; and
the processing methods are cryptographic methods.

3. The portable electronic device of claim 2, wherein
the cryptographic methods include a quantum-resistant
cryptographic method and a cryptographic method other than
20 the quantum-resistant cryptographic method.

4. The portable electronic device of claim 2, wherein
the processor selects one cryptographic method in
accordance with a type of reset requested from the external
device.

25 5. The portable electronic device of claim 2, wherein
the processor selects one cryptographic method in
accordance with a communication condition specified from

the external device.

6. The portable electronic device of claim 5, wherein the processor selects one cryptographic method in accordance with a communication rate specified from the external device.

7. The portable electronic device of claim 5, wherein the processor sets communication systems specified from the external device and selects one cryptographic method in accordance with a communication condition for each of the set communication systems.

8. The portable electronic device of claim 2, wherein the processor transmits information indicating an executable cryptographic method to the external device when executing a command process corresponding to a command from the external device.

9. The portable electronic device of claim 2, wherein upon receiving a command requesting invalidation of a specific cryptographic method from the external device, the processor invalidates the specific cryptographic method.

10. The portable electronic device of claim 2, wherein the processor holds information indicating a cryptographic method being selected, and performs a cryptographic process using the cryptographic method being selected upon receipt of a command requesting a process including the cryptographic process from the external device.

11. The portable electronic device of claim 2, wherein upon receiving a command requesting a process including a

cryptographic process from the external device, the processor selects a cryptographic process to be used for cryptographic processing based on a parameter of the command.

5 12. The portable electronic device of claim 2, wherein upon receiving a command requesting a process including a cryptographic process from the external device, the processor selects a cryptographic method specified by the command.

10 13. An IC card comprising:
 a module including an interface which communicates with an IC card processing device, a memory provided with a storage area which stores data to perform a cryptographic process using each of a plurality of cryptographic methods,
15 and a processor which selects one of the cryptographic methods, shares the selected one of the cryptographic methods with the IC card processing device, and performs a cryptographic process using the cryptographic method shared with the IC card processing device; and
20 a main body including the module.