

IC CARD AND METHOD FOR CONTROLLING IC CARD

BACKGROUND

Field

5 Embodiments of the present invention relate to an integrated circuit (IC) card and a method for controlling the IC card.

Description of Related Art

 In recent years, security attacks targeting personal information have expanded, and ID cards such as bank automatic teller machine (ATM) cards, credit cards, and
10 personal number cards have been transferred to IC cards equipped with IC chips. In this context, IC cards having a function of performing personal authentication using biometric information such as the fingerprints of users who use IC cards are beginning to become widespread. However, in this conventional technology, a large amount of
15 processing time is required for a collation process using biometric information such as fingerprint data.

BRIEF DESCRIPTION OF THE DRAWINGS

 FIG. 1 is a schematic configuration diagram of an IC card 1 according to an embodiment.

20 FIG. 2 is a hardware configuration diagram of the IC card 1 according to the embodiment.

 FIG. 3 is a functional configuration diagram of the IC card 1 according to the embodiment.

 FIG. 4 is a flowchart schematically showing a flow of a process to be executed
25 by an IC chip 20 and a collation processor 60.

FIG. 5 is a sequence diagram showing an example of a process executed by a terminal device 100 and the IC card 1.

FIG. 6 is a sequence diagram showing another example of a process to be executed by the terminal device 100 and the IC card 1.

5

DETAILED DESCRIPTION

An integrated circuit (IC) card of an embodiment includes a communicator, a storage storing biometric authentication information, an acquirer, and a processor. The communicator communicates with a terminal device. The acquirer acquires biometric
10 information of a user. The processor collates the biometric information of the user acquired by the acquirer with the biometric authentication information stored in the storage and stores a collation result into the storage at an activation time.

Hereinafter, an IC card and a method for controlling the IC card according to embodiments will be described with reference to the drawings. Although the IC card of
15 the embodiment is assumed to be a contact type IC card in the following description, a non-contact type IC card may be used.

FIG. 1 is a schematic configuration diagram of an IC card 1 according to the embodiment. For example, the IC card 1 is formed by mounting an IC module 10 on a plastic card base material PT (an example of a card body). That is, the IC card 1
20 includes the IC module 10, a fingerprint sensor 50, a collation processor (collation Pr in FIG. 1) 60, and the card base material PT in which these are embedded. The IC card 1 can communicate with an external terminal device 100 via a contact portion 15. The collation processor 60 authenticates a user by comparing fingerprint information of the user acquired by the fingerprint sensor 50 with biometric authentication information held
25 within the IC module 10 and outputs an authentication result to the IC module 10. The

fingerprint sensor 50 is an example of an “acquirer” for acquiring biometric information and the fingerprint information is an example of the “biometric information.” The biometric information may be vein pattern information, iris information, voice print information, DNA information, or the like as well as fingerprint information. A case in which the collation processor 60 is provided outside the IC module 10 is only an example and the IC module 10 may have a function corresponding to that of the collation processor 60.

For example, the IC card 1 receives a command (a processing request) transmitted by the terminal device 100 via the contact portion 15 and executes processing (command processing) according to the received command. Then, the IC card 1 transmits a response (a processing response) which is a result of executing the command processing to the terminal device 100 via the contact portion 15. The terminal device 100 is a device configured to communicate with the IC card 1, and is, for example, a device including a reader/writer device.

The IC module 10 includes the contact portion 15 and an IC chip 20. For example, the IC module 10 is a module by which a transaction is performed in the form of a chip on tape (COT) in which a plurality of IC modules 10 are arranged on a tape or the like. A single IC module 10 cut out and isolated from the tape may be referred to as a COT.

The contact portion 15 has terminals for various types of signals necessary for the IC card 1 to operate. The terminals for the various types of signals include terminals for supplying a power supply voltage, a clock signal, a reset signal, and the like from the terminal device 100 and a serial data input/output terminal (an SIO terminal) for communicating with the terminal device 100.

The IC chip 20 includes, for example, a large scale integration (LSI) such as a

one-chip microprocessor.

FIG. 2 is a hardware configuration diagram of the IC card 1 according to the embodiment. As shown in FIG. 2, the IC card 1 includes the IC module 10 including the contact portion 15 and the IC chip 20. The IC chip 20 includes a universal
5 asynchronous receiver transmitter (UART) 24, a CPU 25, a read only memory (ROM) 26, a random access memory (RAM) 27, and an electrically erasable programmable ROM (EEPROM) 28. These components are connected via an internal bus BS1.

The UART 24 performs serial data communication with the terminal device 100 via the above-described SIO terminal. The UART 24 outputs data (for example, 1-byte
10 data) obtained by performing parallel conversion on the serial data signal received via the SIO terminal to the internal bus BS1. The UART 24 performs serial conversion on data acquired via the internal bus BS1 and outputs serial data to the terminal device 100 via the SIO terminal. For example the UART 24 receives a command from the terminal
15 device 100 via the SIO terminal. The UART 24 transmits a response to the terminal device 100 via the SIO terminal. The UART 24 is an example of a “communicator.”

The CPU 25 executes a program stored in the ROM 26 or the EEPROM 28 to perform various types of processes of the IC card 1. For example, the CPU 25 executes command processing according to the command received by the UART 24 via the
contact portion 15.

20 The ROM 26 includes, for example, a nonvolatile memory such as a mask ROM. The ROM 26 stores programs for executing various types of processes of the IC card 1 and data such as a command table.

The RAM 27 includes, for example, a volatile memory such as a static RAM (SRAM). The RAM 27 temporarily stores data to be used when various types of
25 processes of the IC card 1 are performed.

The EEPROM 28 includes, for example, an electrically rewritable nonvolatile memory. The EEPROM 28 stores various types of data used by the IC card 1. For example, the EEPROM 28 stores information used for various types of services (applications) using the IC card 1.

5 The collation processor 60 is connected to the internal bus BS1. For example, the collation processor 60 includes a CPU and a program memory. The collation processor 60 is connected to the fingerprint sensor 50 by a dedicated line or the like, and can detect whether or not the fingerprint sensor 50 is in a state in which fingerprint information can be acquired (a power-on state). For example, when the user's finger
10 touches the fingerprint sensor 50 and the fingerprint sensor 50 is powered on, the collation processor 60 determines that the fingerprint sensor 50 is in a state in which fingerprint information can be acquired. The fingerprint sensor 50 acquires the fingerprint information of the user in any one of an electrostatic capacitance type, a thermosensitive type, an optical type, and the like.

15 FIG. 3 is a functional configuration diagram of the IC card 1 according to the embodiment. For example, the IC card 1 includes the above-described UART 24 and fingerprint sensor 50, a processor 30, and a storage 40. For example, the processor 30 includes a biometric information collator 32 and a command processor 34. For example, the command processor 34 is implemented by the CPU 25 executing a program 44.

20 For example, the biometric information collator 32 is implemented by the collation processor 60 executing the program 44. For example, the storage 40 is implemented by a program memory attached to the EEPROM 28 or the collation processor. In the storage 40, the biometric authentication information 42 and the program 44 are pre-stored. The biometric authentication information 42 is information
25 to be collated with the fingerprint information acquired by the fingerprint sensor 50 and

includes information in which a shape pattern of a fingerprint is designated as geometric information, information converted into some feature amount, a combination thereof, or the like. For example, the biometric authentication information 42 includes various types of information extracted from the fingerprint of the user who is an owner of the IC card.

The biometric information collator 32 compares the fingerprint information acquired by the fingerprint sensor 50 with the biometric authentication information 42 pre-stored in the storage 40 and determines that the personal authentication succeeds when these match. For example, "matching" means that a score indicating a degree of matching of information is greater than or equal to a threshold value. When the personal authentication succeeds, the biometric information collator 32 permits access to a secure region in the storage 40 and is brought into a state in which a predetermined process can be executed.

The command processor 34 executes processing (command processing) of various types of commands in accordance with a command (a processing request) transmitted by the terminal device 100. The command processor 34 transmits a response, which is a result of command processing, to the terminal device 100 via the UART 24. With respect to the command processing under a condition of the success of collation (the success of personal authentication), in a case that the authentication success notification is issued from the biometric information collator 32, that is, in a case that access to the secure region in the storage 40 is permitted, the command processor 34 proceeds to perform the process.

FIG. 4 is a flowchart schematically showing a flow of a process to be executed by the IC chip 20 and the collation processor 60. The process of this flowchart is started when the processor 30 (the IC chip 20 and the collation processor 60) and the

fingerprint sensor 50 are activated by supplying electric power to these devices and a RESET signal for an initialization process is received from the terminal device 100.

First, the processor 30 determines whether or not the fingerprint sensor 50 is in a state in which fingerprint information can be acquired (step S100) and transmits request
5 information for requesting transmission of fingerprint information to the fingerprint sensor 50 in a case that it is determined that the fingerprint sensor 50 is in a state in which fingerprint information can be acquired (step S102). In response thereto, the fingerprint sensor 50 transmits the fingerprint information in a predetermined data format and transmission period.

10 Next, the processor 30 waits for the fingerprint information to be transmitted by the fingerprint sensor 50 (step S104) and collates the fingerprint information acquired by the fingerprint sensor 50 with the biometric authentication information 42 pre-stored in the storage 40 when the fingerprint information is transmitted by the fingerprint sensor 50 (step S106).

15 Next, the processor 30 stores a collation result (a personal authentication result) into the storage 40 (step S108) and transmits an answer to reset (ATR) signal as a response to the RESET signal to the terminal device 100 (step S110). Thereby, the process of this flowchart ends.

The collation result (the personal authentication result) stored in the storage 40
20 is assumed to be erased when power supply to the IC card 1 is interrupted and the IC chip 20 or the like is shut down or when power supply to the IC card 1 is restarted and the IC chip 20 or the like is restarted. For example, in a case that the collation result (the personal authentication result) is stored in the RAM 27 of the storage 40, the collation result is erased when power supply is stopped. In a case that the collation result (the
25 personal authentication result) is stored in the EEPROM 28 of the storage 40, the

processor 30 erases the collation result stored in the EEPROM 28 at a reactivation time.

[Biometric authentication during initialization process]

FIG. 5 is a sequence diagram showing an example of a process to be executed by the terminal device 100 and the IC card 1. The present sequence is performed in a situation in which power is supplied from the terminal device 100 to the IC card 1. In the following description, as an example, the IC chip 20 will be described as the command processor 34 and the collation processor 60 will be described as the biometric information collator 32.

First, the terminal device 100 supplies electric power to each of the IC chip 20, the collation processor 60, and the fingerprint sensor 50 of the IC card 1 (steps S200, S202, and S204).

Next, the terminal device 100 transmits a RESET signal to the IC chip 20 (step S206). When the RESET signal is received from the terminal device 100, the IC chip 20 activated by receiving power supply transmits confirmation information for confirming whether or not the fingerprint collation process is possible to the collation processor 60 (step S208).

On the other hand, the collation processor 60 activated by receiving power supply determines whether or not the fingerprint sensor 50 is in a state in which fingerprint information can be acquired on the basis of a power-on state of the fingerprint sensor 50 (step S210).

In a case that it is determined that the fingerprint sensor 50 is in a state in which fingerprint information can be acquired in the processing of S210, the collation processor 60 transmits information indicating the state to the IC chip 20 (step S212). Then, the collation processor 60 transmits request information for requesting transmission of the fingerprint information to the fingerprint sensor 50 in the state in which the fingerprint

information can be acquired (step S214).

When the request information is received, the fingerprint sensor 50 transmits the fingerprint information to the collation processor 60 (step S218).

In a case that it is determined that the fingerprint sensor 50 is in the state in
 5 which the fingerprint information can be acquired, the IC chip 20 reads the biometric authentication information 42 stored in the storage 40 and transmits the biometric authentication information 42 to the collation processor 60 (step S216).

The collation processor 60 collates the biometric authentication information 42 transmitted by the IC chip 20 with the fingerprint information transmitted by the
 10 fingerprint sensor 50 and transmits a collation result (a personal authentication result) to the IC chip 20 and the fingerprint sensor 50 (steps S220 and S222).

Next, when the collation result is received from the collation processor 60, the IC chip 20 stores the received collation result into the storage 40 (step S224). Then, the IC chip 20 transmits the ATR signal to the terminal device 100 by using the UART 24
 15 (step S226).

[Biometric authentication during command processing corresponding to collation command]

FIG. 6 is a sequence diagram showing another example of a process to be executed by the terminal device 100 and the IC card 1. This sequence is performed in a
 20 situation in which a “collation command” is transmitted from the terminal device 100 to the IC card 1 after each device of the IC card 1 is activated. The collation command is, for example, a command transmitted when a user who uses the IC card 1 performs personal authentication in response to a request from the terminal device 100 side.

First, the terminal device 100 transmits the collation command to the IC chip 20
 25 (the command processor 34) of the IC card 1 (step S300).

Next, the IC chip 20 determines whether or not the collation result is stored in the storage 40 (step S302) and executes command processing corresponding to the collation command in accordance with the collation result by omitting the above-described fingerprint collation process when it is determined that the collation
5 result is stored in the storage 40 (step S304). Then, the IC chip 20 transmits a response, which is a command processing result, to the terminal device 100 via the UART 24 (step S306).

For example, in a case that the collation result is “mismatching,” that is, in a case that the personal authentication fails, the IC chip 20 transmits error information or
10 the like as a response to the terminal device 100 without proceeding to perform the process. On the other hand, in a case that the collation result is “matching,” that is, in a case that the personal authentication succeeds, the IC chip 20 proceeds to perform the command processing.

On the other hand, in a case that it is determined that the collation result is not
15 stored in the storage 40, the IC chip 20 transmits confirmation information for confirming whether or not the fingerprint collation process is possible to the collation processor 60 (the biometric information collator 32) (step S304) and starts the above-described fingerprint collation process. For example, the collation result is not stored in the storage 40 in a case that a finger is not placed on the fingerprint sensor 50 at
20 the time of activation of the IC chip 20 or the like and a processing time is timed out. In this case, the IC chip 20 starts the fingerprint collation process.

Next, the collation processor 60 determines whether or not the fingerprint sensor 50 is in a state in which fingerprint information can be acquired on the basis of the power-on state of the fingerprint sensor 50 (step S310). In a case that it is determined
25 that the fingerprint sensor 50 is in a state in which fingerprint information can be

acquired, the collation processor 60 transmits information indicating the state to the IC chip 20 (step S312).

Next, in a case that it is determined that the fingerprint sensor 50 is in a state in which fingerprint information can be acquired, the IC chip 20 reads biometric authentication information 42 stored in the storage 40 and transmits the biometric authentication information 42 to the collation processor 60 (step S314).

On the other hand, the collation processor 60 transmits request information for requesting transmission of the fingerprint information to the fingerprint sensor 50 in the state in which the fingerprint information can be acquired (step S316). When the request information is received, the fingerprint sensor 50 transmits the fingerprint information to the collation processor 60 (step S318).

Next, the collation processor 60 collates the biometric authentication information 42 transmitted by the IC chip 20 with the fingerprint information transmitted by the fingerprint sensor 50 and transmits a collation result (a personal authentication result) to the IC chip 20 and the fingerprint sensor 50 (steps S320 and S322).

Next, when the collation result is received from the collation processor 60, the IC chip 20 stores the collation result into the storage 40 (step S324). Then, the IC chip 20 executes command processing corresponding to a collation command on the basis of the collation result stored in the storage 40 in the processing of S324 as the processing of S304 described above.

Although an example in which the IC chip 20 (the command processor 34) and the collation processor 60 (the biometric information collator 32) perform the fingerprint collation process in a case that it is determined that the collation result is not stored in the storage 40 as the processing result of S302 has been described in the above-described embodiment, the present invention is not limited thereto. For example, the IC chip 20

(the command processor 34) and the collation processor 60 (the biometric information collator 32) may perform the fingerprint collation process in a case that the collation result is stored in the storage 40 and it is determined that the collation result is “mismatching” or “failure of personal authentication” after it is determined whether or not the collation result is “matching” or “success of personal authentication.” The collation result of “matching” or “success of personal authentication” is an example of a “predetermined condition.” Thus, the personal authentication can be performed twice at an activation time and at a collation command time.

Although an example in which the IC chip 20 (the command processor 34) and the collation processor 60 (the biometric information collator 32) perform the fingerprint collation process at the activation time has been described in the above-described embodiment, the present invention is not limited thereto. For example, the IC chip 20 (the command processor 34) and the collation processor 60 (the biometric information collator 32) may perform the fingerprint collation process when a command processing corresponding to a SELECT (SELECT [by DF name]) command is performed. The SELECT command is a command for designating a predetermined file (a dedicated file) of an application stored in the storage 40 and is a command received from the terminal device 100 before at least the collation command. The SELECT command is an example of a “predetermined command”.

According to at least one embodiment described above, there are provided a storage (40) storing biometric authentication information (42); an acquirer (the fingerprint sensor 50) configured to acquire biometric information (fingerprint information) of the user; and a processor (30) configured to collate the biometric information of the user acquired by the acquirer with the biometric authentication information stored in the storage and store a collation result into the storage at an

activation time, thereby shortening a processing time required for personal authentication because a process of collating the biometric information is executed at a timing earlier than a timing at which a collation command in which the collation of the biometric information is required is received.

5 The above-described embodiment can be represented as follows.

 An integrated circuit card including:

 a communicator configured to communicate with a terminal device;

 a storage storing biometric authentication information;

 an acquirer configured to acquire biometric information of a user; and

10 a hardware processor configured to execute a program stored in the storage,

 wherein the processor is configured to execute a process of collating the

 biometric information of the user acquired by the acquirer with the biometric

 authentication information stored in the storage and store a collation result into the

 storage at an activation time by executing the program.

15 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 embodiments described herein may be embodied in a

 variety of other forms; furthermore, various omissions, substitutions and changes in the

 form of the embodiments described herein may be made without departing from the spirit

20 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.

What is claimed is:

1. An integrated circuit card comprising:

a communicator configured to communicate with a terminal device;

5 a storage storing biometric authentication information;

an acquirer configured to acquire biometric information of a user; and

a processor configured to collate the biometric information of the user acquired
by the acquirer with the biometric authentication information stored in the storage and
store a collation result into the storage at an activation time.

10

2. The integrated circuit card according to Claim 1, wherein

the processor is configured to:

determine whether or not the collation result has been stored in the storage in a case that
the communicator receives a collation command from the terminal device at a time

15 different from the activation time;

perform command processing on the basis of the collation result in a case that
the processor determines that the collation result has been stored in the storage; and

transmit a response according to the command processing to the terminal device
using the communicator.

20

3. The integrated circuit card according to Claim 2, wherein

the processor is configured not to perform a collation process as a part of the command
processing associated with the collation command in a case that the communicator
receives the collation command from the terminal device and the processor determines

25 that the collation result is stored in the storage.

4. The integrated circuit card according to Claim 2 or 3, wherein

the processor is configured to:

perform a collation process as a part of the command processing associated with the

5 collation command in a case that the processor determines that the collation result has not
been stored in the storage; and

perform the command processing based on a result of performing the collation
process and store the collation result into the storage.

10 5. The integrated circuit card according to Claim 2 or 3, wherein

the processor is configured to:

further determine whether or not the collation result satisfies a predetermined condition
in a case that the processor determines that the collation result has been stored in the
storage;

15 perform a collation process as a part of the command processing associated with
the collation command in a case that the processor determines that the collation result
does not satisfy the predetermined condition; and

perform the command processing on the basis of a result of performing the
collation process and store the collation result into the storage.

20

6. The integrated circuit card according to any one of Claims 2 to 5, wherein

the processor is configured to perform a collation process as a part of a command

processing associated with a predetermined command received before the collation

command at other than the activation time in a case that the processor determines that the

25 collation result has not been stored in the storage.

7. A method for controlling an integrated circuit card comprising a processor, a communicator configured to communicate with a terminal device, a storage storing biometric authentication information, and an acquirer configured to acquire biometric information of a user, the method comprising:

collating, by the processor, the biometric information of the user acquired by the acquirer with the biometric authentication information stored in the storage and storing a collation result into the storage at an activation time.

8. An integrated circuit card comprising:

an acquirer configured to acquire biometric information of a user;

an integrated circuit module comprising a communicator configured to communicate with a terminal device, a storage storing biometric authentication information, and a processor configured to collate the biometric information of the user acquired by the acquirer with the biometric authentication information stored in the storage and store a collation result into the storage at an activation time; and

a card base material in which the acquirer and the integrated circuit module are embedded.

9. The integrated circuit card according to Claim 8, wherein

hardware configured to perform a collation process among processes to be performed by the processor is provided outside the integrated circuit module, and the acquirer, the integrated circuit module, and the hardware are embedded in the card base material.