

PORTABLE ELECTRONIC APPARATUS, CONTROL METHOD FOR
PORTABLE ELECTRONIC APPARATUS, AND IC CARD

FIELD

Embodiments described herein relate generally to a
5 portable electronic apparatus configured to achieve
various kinds of processing by, for example,
transmitting and receiving commands.

BACKGROUND

In general, an IC card for use as a portable
10 electronic apparatus is provided with a card-shaped
main body of plastic or the like and an IC module
embedded therein. The IC module comprises an IC chip.
The IC chip comprises a nonvolatile memory, such as an
electrically erasable programmable read-only memory
15 (EEPROM) or flash ROM, which can hold data without
power supply, and a CPU configured to perform various
operations.

IC cards are highly portable and can perform
communication with external equipment and complicated
20 arithmetic processing. Since they are hard to forge,
moreover, the IC cards are assumed to be loaded with
highly confidential information or the like and used
for a security system, electronic business transaction,
etc.

25 In recent years, non-contact IC cards capable of
data transmission and reception by non-contact
communication have become widely used. One such

non-contact IC card comprises an IC chip and antenna.
This IC card receives a magnetic field generated from a
card reader/writer of a terminal device that processes
the IC card and is activated as the antenna therein is
5 excited by electromagnetic induction.

According to its protocol specifications, the non-
contact IC card transitions to a standby state in which
a wake-up command (WUPA or WUPB) is awaited in response
to an instruction (DESELECT) for a transition to a
10 state in which processing is interrupted after the card
is activated to perform an operation. The transition
to this standby state is an operation of a protocol
layer.

There are various cases where processing is
15 interrupted so that the non-contact IC card is shifted
to an inactive state by a Deselect command. In one
such case, the interruption is temporary and processing
having hitherto been performed is continued at the
restart. In another case, previous processing is reset
20 and new processing is started from an initial state.
These cases are selected depending on the state to
which a transition is to be made from the OS or
application state. Since the processing for the
transition to the inactive state by the Deselect
25 command is the operation of the protocol layer,
however, no operations are provided corresponding to
the above-described various cases.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram showing an exemplary configuration of an IC card system that handles a non-contact IC card for use as a portable electronic apparatus according to an embodiment;

FIG. 2 is a diagram showing an exemplary configuration of the non-contact IC card according to the embodiment;

FIG. 3 is a diagram showing an exemplary configuration of a block prescribed by a transfer protocol for non-contact communication according to the embodiment;

FIG. 4 is a diagram showing an exemplary configuration of a PCB according to the embodiment;

FIG. 5 is a diagram showing an exemplary combination of RFU1 and RFU2 and exemplary processing contents according to the embodiment;

FIG. 6 is an exemplary flowchart showing the operation of the non-contact IC card performed when a DESELECT command is received according to the embodiment;

FIG. 7 is an exemplary flowchart showing the operation of a non-contact IC card of a second embodiment performed when a DESELECT command is received;

FIG. 8 is an exemplary diagram showing the correspondence between a flag and a region stored with

information on the OS state according to the
embodiment;

FIG. 9 is an exemplary diagram showing the
correspondence between a flag and a region stored with
5 information on the application state according to the
embodiment; and

FIG. 10 is an exemplary flowchart showing the
operation of a non-contact IC card of a third
embodiment performed when a DESELECT command is
10 received.

DETAILED DESCRIPTION

In general, according to one embodiment, a
portable electronic apparatus comprising: a receiving
section configured to receive from an external device
15 an instruction for a transition from an active state to
a state in which processing is temporarily interrupted;
a recognition section configured to recognize a
processing method in a state established in the active
state based on processing specification information
20 contained in the instruction; and a controller
configured to maintain the state established in the
active state even in the state for the temporary
interruption or restore an initial state before the
establishment.

25 [First Embodiment]

A portable electronic apparatus according to a
first embodiment of the present invention will now be

described in detail with reference to the accompanying drawings.

FIG. 1 is a diagram showing an exemplary configuration of an IC card system that handles a non-
5 contact IC card for use as a portable electronic apparatus according to an embodiment.

The IC card system comprises a non-contact IC card 101, card reader/writer 102, terminal device 103, keyboard 104, display 105, and printer 106.

10 The terminal device 103 connects with the card reader/writer 102, keyboard 104, display 105, and printer 106. The IC card 101 is connected to the terminal device 103 through the card reader/writer 102 as an external device.

15 The non-contact IC card 101 transitions to an operable state when it is supplied with energy from the card reader/writer 102. Various kinds of processing are performed in response to request commands transmitted from the card reader/writer 102.

20 The terminal device 103 comprises a personal computer or the like. The terminal device 103 performs the various kinds of processing by executing various control programs stored in its built-in memory. Data are transferred to and from the non-contact IC card 101
25 via the card reader/writer 102.

FIG. 2 is a diagram showing an exemplary configuration of the non-contact IC card according to

the embodiment.

The non-contact IC card 101 comprises a CPU 201, data memory 202, working memory 203, program memory 204, timers 205, and communication section 206.

5 A section (including the CPU 201, data memory 202, working memory 203, program memory 204, and timers 205) enclosed by broken line in FIG. 2 comprises a single IC chip 200 (or a plurality of such chips). The IC chip 200 and communication section 206 are connected and
10 integrated into an IC module, which is embedded in the main body of the non-contact IC card.

 The CPU 201 is a controller that performs various data processing operations, such as various decision and determination processing operations, memory writing
15 and reading, etc.

 The data memory 202 is a rewritable nonvolatile memory, such as an EEPROM, which stores various data including application data in a file structure.

 The working memory 203 is a volatile memory, such
20 as a random access memory (RAM), which temporarily holds processing data processed by the CPU 201.

 The program memory 204 is a non-rewritable fixed memory, such as a mask read-only memory (ROM), which is stored with control programs of the CPU 201.

25 The timers 205 count fixed time periods. These timers are correlated with logical channels and are at least as many as the logical channels.

The communication section 206 is an antenna unit, which receives a modulated wave from the card reader/writer 102 in a non-contact manner or originates a modulated wave to the outside. Further, the communication section 206 produces energy or clocks to be supplied to an internal circuit from the received modulated wave.

The following is a description of the operation of the non-contact IC card 101 of the present embodiment.

As mentioned before, the card reader/writer 102 generates a magnetic field to excite the non-contact IC card 101 within a communication range by electromagnetic induction. If a plurality of IC cards exist within the communication range, a "collision" may occur such that the terminal device 103 cannot correctly identify the IC cards in an initial response. In order to prevent this collision and to ensure correct identification of the IC cards, the terminal device 103 and non-contact IC card 101 cooperate with each other to perform anti-collision processing.

After the anti-collision processing is finished, the non-contact IC card 101 transitions to an active state and transmits or receives commands prescribed by ISO/IEC 7816.

If the terminal device 103 temporarily interrupts communication with the active non-contact IC card 101 in order to start communication with another

non-contact IC card 101, a DESELECT command is transmitted from the card reader/writer 102 to the active IC card 101. Thereupon, the IC card 101 concerned transitions from the active state to an inactive state in which the processing is temporarily interrupted.

The DESELECT command is prescribed by the following ISO/IEC 14443 Supervisory Block.

FIG. 3 is a diagram showing an exemplary configuration of a block prescribed by a transfer protocol for non-contact communication according to the embodiment. The block comprises a prologue field, information field, and epilogue field. A protocol control byte (PCB) is essential data used to select necessary information for the control of data transfer. The information field is not used as an instruction for inactivation (DESELECT).

FIG. 4 is a diagram showing an exemplary configuration of the PCB according to the embodiment.

Two leftmost bits "11" indicate that the data concerned is information used for communication between the card reader/writer 102 and non-contact IC card 101. Next two bits "00" are indicative of the DESELECT command.

If the fifth bit as counted from the leftmost one is "1", then it indicates that a card identifier (CID) exists in the prologue field. Two rightmost bits in

FIG. 4 are RFU bits reserved for future use.

If the processing is temporarily interrupted by the DESELECT command, according to the present embodiment, two bits RFU1 and RFU2 are used to specify
5 whether to maintain a state established in the active state or to restore an initial state before the establishment.

FIG. 5 is a diagram showing an exemplary combination of RFU1 and RFU2 and exemplary processing
10 contents according to the embodiment.

If RFU1 is 1, the operating system (OS) is restored to its initial state. If RFU1 is 0, the current OS state is maintained. If RFU2 is 1, the application is restored to its initial state. If RFU2
15 is 0, the current application state is maintained. The OS and application states will be described later.

FIG. 6 is an exemplary flowchart showing the operation of the non-contact IC card 101 performed when the DESELECT command is received according to the
20 embodiment.

In Step 502, RFU1 of the PCB is checked to see if it is 1. If the decision in Step 502 is YES, that is, if RFU1 is 1, processing is performed to restore the OS to the initial state. Information indicative of the OS
25 state to be processed includes, for example, the following items.

"Matching state information" indicates a flag

state in which the non-contact IC card 101 is key-matched.

5 "Current EF information" is information as to whether or not an elementary file (EF) is selected by a SELECT command.

 "Current DF information" is information as to whether or not a dedicated file (DF) is selected by the SELECT command.

10 "Current record information" is information on a current record.

 "Logical channel information" is information on a currently open logical channel.

 All these OS conditions are saved in the working memory 203.

15 After Step 503 is performed or if the decision in Step 502 is NO, that is, if RFU1 is 0, RFU2 is checked in Step 504 to see if it is 1.

 If the decision in Step 504 is YES, that is, if RFU2 is 1, processing is performed in Step 505 to
20 restore the application to the initial state.
 Information indicative of the application state to be processed includes, for example, the following items.

 "State transition management information" is
25 information on the progress of a series of processing flows.

 "Authentication/matching state management information" is information indicative of

authentication and matching states managed within the application and used besides the OS to manage the authentication and matching states.

5 "Session key information" is information on different keys that are generated by the application based on random numbers on each occasion.

 "Secret information" is information that is not output from the card managed within the application.

10 All these application conditions are saved in the working memory 203.

 After Step 505 is performed or if the decision in Step 504 is NO, that is, if RFU2 is 0, a transition is made to a halt state in Step 506. This state is maintained until a wake-up command is issued anew.

15 [Second Embodiment]

 A second embodiment differs from the first embodiment in that the OS or application state to which a transition is to be made can be specified on each occasion. Therefore, like numbers are used to designate like portions of the first and second
20 embodiments and a detailed description thereof is omitted.

 FIG. 7 is an exemplary flowchart showing the operation of a non-contact IC card 101 of the second
25 embodiment performed when a DESELECT command is received.

 In Step 602, RFU1 of a PCB is checked to see if it

is 1. If the decision in Step 602 is YES, that is, if RFU1 is 1, information on a region specified by a flag is restored to its initial state in Step 603.

For example, if each bit of flag is 1, information
5 indicative of each corresponding OS state is restored to its initial state. If each bit is 0, the information indicative of each corresponding OS state is maintained.

FIG. 8 is an exemplary diagram showing the
10 correspondence between a flag 401 and a region stored with information on the OS state according to the embodiment.

Since flag 401 is set to "10110" in FIG. 8,
"matching state information", "current DF information",
15 and "current record information" are restored to their initial states, while "current EF information" and "logical channel information" are maintained as they are.

After Step 603 is performed or if the decision in
20 Step 602 is NO, that is, if RFU1 is 0, RFU2 is checked in Step 604 to see if it is 1.

If the decision in Step 604 is YES, that is, if RFU2 is 1, processing is performed in Step 605 to
25 restore the application specified by a flag to its initial state.

For example, if each bit of flag is 1, information indicative of each corresponding application state is

restored to its initial state. If each bit is 0, the information indicative of each corresponding application state is maintained.

FIG. 9 is an exemplary diagram showing the correspondence between a flag 402 and a region stored with information on the application state according to the embodiment.

Since flag 402 is set to "1100" in FIG. 9, "state transition management information" and "authentication/matching state management information" are restored to their initial states, while "session key information" and "secret information" are maintained as they are.

After Step 605 is performed or if the decision in Step 604 is NO, that is, if RFU2 is 0, a transition is made to a halt state in Step 606. This state is maintained until a wake-up command is issued anew.

Flags 401 and 402 are set when the non-contact IC card 101 is issued. After the issue, flags 401 and 402 may be made either rewritable or non-rewritable.

[Third Embodiment]

A third embodiment differs from the second embodiment in that the OS or application state to which a transition is to be made can be specified on each occasion not by a PCB but by flags. Therefore, like numbers are used to designate like portions of the second and third embodiments and a detailed description

thereof is omitted.

FIG. 10 is an exemplary flowchart showing the operation of a non-contact IC card 101 of the third embodiment performed when a DESELECT command is received.

In Step 701, the non-contact IC card 101 restores information on a region specified by the flag. Since this operation resembles the one described with reference to FIG. 8, a repeated description thereof is omitted.

In Step 702, the non-contact IC card 101 restores information on the region specified by the flag. Since this operation resembles the one described with reference to FIG. 9, a repeated description thereof is omitted.

A transition is made to a halt state in Step 703, and this state is maintained until a wake-up command is issued anew.

Flags 401 and 402 are set when the non-contact IC card 101 is issued. After the issue, flags 401 and 402 may be made either rewritable or non-rewritable.

The functions explained in connection with the embodiments described herein are not limited to configurations based on hardware, and they can be realized by loading a computer with programs that contain them by means of software. Further, each function may be appropriately constructed by selecting

either software or hardware.

The present invention is not limited directly to the embodiments described herein, and in carrying out the invention, its constituent elements may be embodied
5 in various forms without departing from the spirit of the invention.

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
10 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 of the
15 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.

- 16 -

WHAT IS CLAIMED IS:

1. An IC card comprising:

a receiving section configured to receive from an external device an instruction for a transition from an active state to a state in which processing is temporarily interrupted;

a recognition section configured to recognize a processing method in a state of each of an OS and an application which is established in the active state based on processing specification information contained in the instruction;

a storage section stored with individual information configured to determine whether to maintain the state established in the active state for each of individual objects as subdivisions of the state of each of the OS and the application even in the state for the temporary interruption or to restore an initial state before the establishment; and

a controller which performs processing, determined for the individual objects by the individual information, with respect to the state of each of the OS and the application for which the processing specification information specifies the restoration of the state established in the active state to the initial state before the establishment,

wherein each of the individual objects of the OS includes at least one of a flag state in which the IC card is key-matched, information as to whether or not an EF or a

- 17 -

DF is selected by a command, information on a current record, and information on a currently open logical channel,

wherein each of the individual objects of the application includes at least one of information on the progress of a series of processing flows, information indicative of authentication and matching states managed within the application, information on different keys generated based on random numbers, and information that is not output from the IC card managed within the application.

2. An IC card comprising:

a receiving section configured to receive from an external device an instruction for a transition from an active state to a state in which processing is temporarily interrupted;

a storage section stored with individual information which determines whether to maintain the state of each of an OS and an application which is established in the active state to be processed even in the state for the temporary interruption or to restore an initial state before the establishment; and

a controller configured to perform processing determined for the state of each of the OS and the application by the individual information,

wherein each of the individual objects of the OS includes at least one of a flag state in which the IC card

- 18 -

is key-matched, information as to whether or not an EF or a DF is selected by a command, information on a current record, and information on a currently open logical channel,

5 wherein each of the individual objects of the application includes at least one of information on the progress of a series of processing flows, information indicative of authentication and matching states managed within the application, information on different keys
10 generated based on random numbers, and information that is not output from the IC card managed within the application.

3. A control method for an IC card, comprising:

receiving from an external device an instruction for a transition from an active state to a state in which
15 processing is temporarily interrupted;

recognizing a processing method in a state of each of an OS and an application which is established in the active state based on processing specification information contained in the instruction;

20 storing individual information which determines whether to maintain the state established in the active state for each of individual objects as subdivisions of the state of each of the OS and the application even in the state for the temporary interruption or to restore an
25 initial state before the establishment; and

performing processing, determined for the individual

- 19 -

objects by the individual information, with respect to the state of each of the OS and the application for which the processing specification information specifies the restoration of the state established in the active state to
5 the initial state before the establishment,

wherein each of the individual objects of the OS includes at least one of a flag state in which the IC card is key-matched, information as to whether or not an EF or a DF is selected by a command, information on a current
10 record, and information on a currently open logical channel,

wherein each of the individual objects of the application includes at least one of information on the progress of a series of processing flows, information
15 indicative of authentication and matching states managed within the application, information on different keys generated based on random numbers, and information that is not output from the IC card managed within the application.

4. A control method for an IC card, comprising:
20 receiving from an external device an instruction for a transition from an active state to a state in which processing is temporarily interrupted;

storing individual information which determines whether to maintain the state of each of an OS and an
25 application which is established in the active state to be processed even in the state for the temporary interruption

- 20 -

or to restore an initial state before the establishment;
and

performing processing determined for the state of each
of the OS and the application by the individual

5 information,

wherein each of the individual objects of the OS
includes at least one of a flag state in which the IC card
is key-matched, information as to whether or not an EF or a
DF is selected by a command, information on a current
10 record, and information on a currently open logical
channel,

wherein each of the individual objects of the
application includes at least one of information on the
progress of a series of processing flows, information
15 indicative of authentication and matching states managed
within the application, information on different keys
generated based on random numbers, and information that is
not output from the IC card managed within the application.

5. An IC card comprising:

20 an IC module comprising a receiving section configured
to receive from an external device an instruction for a
transition from an active state to a state in which
processing is temporarily interrupted, a recognition
section configured to recognize a processing method in a
25 state of each of an OS and an application which is
established in the active state based on processing

specification information contained in the instruction, a storage section stored with individual information which determines whether to maintain the state established in the active state for each of individual objects as subdivisions
5 of the state of the OS and the application even in the state for the temporary interruption or to restore an initial state before the establishment, and a controller configured to perform processing, determined for the individual objects by the individual information, with
10 respect to the state of the OS and the application for which the processing specification information specifies the restoration of the state established in the active state to the initial state before the establishment; and
an IC card main body which contains the IC module,
15 wherein each of the individual objects of the OS includes at least one of a flag state in which the IC card is key-matched, information as to whether or not an EF or a DF is selected by a command, information on a current record, and information on a currently open logical
20 channel,
wherein each of the individual objects of the application includes at least one of information on the progress of a series of processing flows, information indicative of authentication and matching states managed
25 within the application, information on different keys generated based on random numbers, and information that is

- 22 -

not output from the IC card managed within the application.

6. An IC card comprising:

an IC module comprising a receiving section configured to receive from an external device an instruction for a transition from an active state to a state in which processing is temporarily interrupted, a storage section stored with individual information which determines whether to maintain the state of each of an OS and an application which is established in the active state to be processed even in the state for the temporary interruption or to restore an initial state before the establishment, and a controller configured to perform processing determined for the state of each of the OS and the application by the individual information; and

an IC card main body which contains the IC module, wherein each of the individual objects of the OS includes at least one of a flag state in which the IC card is key-matched, information as to whether or not an EF or a DF is selected by a command, information on a current record, and information on a currently open logical channel,

wherein each of the individual objects of the application includes at least one of information on the progress of a series of processing flows, information indicative of authentication and matching states managed within the application, information on different keys

- 23 -

generated based on random numbers, and information that is not output from the IC card managed within the application.