

DESCRIPTION

Data Communication System, Data Communication
Method, and Data Communication Apparatus

5

TECHNICAL FIELD

[0001]

The present invention relates to a data
communication system, a data communication method and a
10 data communication apparatus that are adapted to effect
data communication between data communication apparatuses
provided with relatively large capacity memory areas,
particularly, to a data communication system, a data
communication method and a data communication apparatus
15 that are adapted to effect data communication between
data communication apparatuses adapted to transmit
encrypted data through contactless interfaces.

[0002]

In more detail, the present invention relates to a
20 data communication system, a data communication method
and a data communication apparatus that are adapted to
transfer value information such as electronic money and
an electronic ticket between data communication
apparatuses having contactless interfaces, particularly,
25 a data communication system, a data communication method
and a data communication apparatus that are adapted to
transfer data between data communication apparatuses
having contactless interfaces, while preventing the data
from being duplicated in a data transfer source and a
30 data transfer destination.

BACKGROUND ART

[0003]

A contactless or proximity communication system typically available in the form of an IC card is widespread by reason of its operational easiness. For instance, pre-storing of password codes and other personal authentication information and/or value information such as an electronic ticket in the IC card is adaptable to provide processing for authentication of visitors or passengers in places such as cash dispensers, concert hall gateways and ticket wickets at a station.

[0004]

Radio communication of this type is generally realized on the basis of a principle of electromagnetic induction. That is, a system is configured with an IC card having a memory function and a card reader/writer performing read/write access to a memory of the IC card is required, and an IC card-side loop coil serving as a primary coil and a card reader/writer-side antenna serving as a secondary coil form a transformer unit as a system. Then, an electromagnetic induction action is adapted to transmit power and information similarly from the card reader/writer side to the IC card, causing the IC card side to be driven with the fed power for giving an answer to a question signal from the card reader/writer side. Thus, it is not necessary for the IC card itself to have a drive power supply such as a battery.

[0005]

A general way to make use of the IC card is putting the IC card over the card reader/writer by a user. The card reader/writer side keeps up polling to the IC card

at all times, so that if an external IC card is detected, communication operation between the IC card and the card reader/writer is started (See a non-patent document 1, for instance).

5 [0006]

In recent years, in cooperation also with an improvement on a micro-fabrication technology, an IC card having a relatively large capacity memory comes into existence. According to an IC card with a large capacity
10 memory, it is possible to expand a file system on a memory space and to store more than one application simultaneously, permitting a single IC card to be used for more than one purpose. For instance, storing of more than one application, such as the electronic money for
15 electronic payment and the electronic ticket for admission to a specific concert hall, on a single IC card makes it possible to apply the single IC card for various purposes. Terms of the electronic money and the electronic ticket specified herein are referred to a
20 mechanism required for settlement of accounts (or the electronic payment) through electronic data issued depending on a fund provided by a user or to the above electronic data itself.

[0007]

25 The general way to make use of the IC card is putting the IC card over the card reader/writer by the user. The card reader/writer side keeps up the polling to the IC card at all times, so that if an external IC card is detected, communication operation between the IC
30 card and the card reader/writer is started.

[0008]

At this time, personal identification or authentication processing between the IC card and the IC card reader/writer is performed by matching a secret number input to an IC card reader side by a user with a secret number stored on the IC card. (The secret number used at the time of IC card access is particularly referred to as a PIN (Personal Identification Number)). Then, when the personal identification or authentication processing results in success, the user is allowed to use the application contained in the IC card, that is, to access to a service memory area assigned to the application (the memory area assigned to the application is referred to as "the service memory area"). The access to the service memory area requires suitably encrypted communication depending on an application security level.

[0009]

Further, the IC card or the card reader/writer (or a card read/write apparatus) permits a wired interface (not shown) for connection to an external apparatus to be included, in addition to the radio or contactless interface, leading to mounting of IC card and reader/writer functions or one or both of the IC card and card reader/writer functions to each device of a mobile phone, a PDA (Personal Digital Assistance), a CE (Consumer Electronics) apparatus and a personal computer etc. In such a case, it is possible to make use of an IC card technology as a versatile two-way proximity communication interface.

[0010]

For instance, when apparatuses themselves such as computers and information household electronic

apparatuses are combined to form the proximity communication system, the contactless communication involving use of the IC card is effected in the form of one-to-one communication. Alternatively, it is also allowable for a certain apparatus to communicate also with a mating device other than the apparatus such as the contactless IC card, in which case, one application adapted to effect one-to-multiple communication in one apparatus and a plurality of cards is also supposed to be available.

[0011]

Further, running of various types of applications involving use of the IC card, such as an exchange of electronic value information with the outside as well as the electronic payment, is attainable on an information processing terminal. For instance, use of a user interface such as a keyboard and a display on the information processing terminal permits user interaction with the IC card to be effected on the information processing terminal. Further, connection between the IC card and the mobile phone permits stored contents in the IC card to be exchanged over a telephone network. Furthermore, establishment of connection from the mobile phone to the Internet is adaptable to pay a charge for service with the IC card.

[0012]

As described the above, a useful service based on the contactless or proximity communication is realizable as a substitute for a conventional prepaid card or a service card available on a shop-by-shop basis by assigning a file system for a certain service source

provider to a built-in memory of an IC card, before
managing, within the assigned file system, information
(such as user identification or authentication
information, remaining value information and a history
5 (or a log) of service used) for service operations by the
concerned provider.

[0013]

Conventionally, the IC card has been issued
individually on a service source provider-by-service
10 source provider basis, providing the service for the user.
Thus, the user has been required to carry with an
assortment of IC cards for each desired service. To the
contrary, according to an IC card having a relatively
large capacity memory space, it is effective in making
15 sure of a sufficient capacity as much as that adaptable
to record information relating to more than one service
in a built-in memory of a single IC card.

[0014]

Referring now to a prepaid-type voucher such as a
20 prepaid card, there is an enactment of "a law relating to
prepaid card-type voucher regulations etc." (which goes
by the name of "a prepaid card law") for imposing
required regulations for registrations and others upon
prepaid-type voucher issuers mainly with the object of
25 securing appropriate administrations for services such as
issuance of the prepaid-type vouchers so as to protect
the profits of those including prepaid-type voucher
purchasers and also to keep up the credit with respect to
the prepaid-type vouchers, wherein there exists
30 obligations to give a description of prescribed matters
such as a logo and a reference to a prepaid card surface

(or a voucher surface) for the sake of convenience of the user and/or keeping of a distribution order etc. (See Section 12 of the above law).

[0015]

- 5 When the prepaid card is materialized by storing prepayment information in an IC card memory function, required information regulated by the law needs to be printed on a medium, resulting in a limitation of an available service to a single service. To the contrary,
- 10 when the IC card function is put into use on a display function-mounted mobile terminal like the mobile phone, displaying of information relating to desired value information on the display (See a patent document 1, for instance) is adaptable to meet the regulations in the
- 15 above law, permitting sharing by more than one service source provider to be attained. Thus, the service source provider gets relief from a burden on the card issuance, while the user may bring a reduction in number of IC cards to be carried under management to realization.

20 [0016]

[Patent document 1]

Japanese Patent Application Publication (KOKAI)
2003-141434

[Non-patent document 1]

- 25 "RFID handbook, Principles and Applications of Contactless IC Card" by Klaus Finkenzeller (Nikkan Kogyou Shimbun Ltd., ISBN 4-526-0470105)

[Disclosure of the Invention]

Problems Solved by the Invention

30 [0017]

As described the above, various types of value

information such as the electronic money and the electronic ticket may be stored on an IC card or an IC chip in security.

[0018]

5 An increasing progressive spread of the IC card in the future is supposed to bring about a situation in which each user is required to possess two or more IC cards (or IC chip-mounted apparatuses). With considerations of convenience for the user, such an IC
10 card service environment gives rise to the need for transfer of data contained in the IC card.

[0019]

 The transfer of data specified herein includes not only IC card-to-IC card transfer but also transfer of
15 data from the IC card to the IC chip-mounted apparatus (such as the mobile phone and other types of mobile apparatuses) and transfer of data from one IC chip-mounted apparatus to the other. For the sake of convenience, the IC card and the IC chip-mounted
20 apparatus are hereinafter altogether referred to as the IC card.

[0020]

 The data serving herein as the transfer target is available in the form of value information such as the
25 electronic money and the electronic ticket. This is just as the user is required to transfer contents in purses properly used for each purpose or to make integration into one purse.

[0021]

30 In a case of transferring cash, the transfer from one purse to the other is involved, whereas no additional

cash is gained. To the contrary, while the value information such as the electronic money and the electronic ticket is valuable as much as the cash, its entity is given in the form of digital data, so that at
5 the time of the data transfer, one possibility may exist that original value information will be present in an overlapped state in both of a data transfer source IC card and a data transfer destination IC card. If the situation as described above occurs, the value
10 information provider is obliged to provide a service beyond one's actually issued service or an overlapped service, resulting in detriment to one's interests.
[0022]

A communication path adapted to establish the
15 connection between the IC cards with the contactless interfaces is available in the form of an encrypted transmission path of safety, resulting in no danger of causing the data to be overlapped by a leakage to the outside in the process of the data transfer. On the
20 other hand, an inter IC-card connection state is maintained with both the IC cards spaced at a relatively short distance serving as a communication range in the contactless interfaces, so that one possibility may exists that the data will be overlapped when some
25 unexpected accidents cause the IC cards to be pulled apart, leading to a cut of the connection, or when the contactless communication results in no normal termination by other causes.

[0023]

30 The present invention has been undertaken in view of the above technical problems and is mainly intended to

provide a data communication system, a data communication method and a data communication apparatus that are excellent and adaptable to effect data communication between data communication apparatuses adapted to
5 transmit encrypted data through contactless interfaces.
[0024]

The present invention is further intended to provide a data communication system, a data communication method and a data communication apparatus that are
10 excellent and adaptable to suitably transfer value information such as electronic money and an electronic ticket between data communication apparatuses having contactless interfaces.
[0025]

15 The present invention is still further intended to provide a data communication system, a data communication method and a data communication apparatus that are excellent and adaptable to transfer data between data communication apparatuses having contactless interfaces
20 while preventing the data from being overlapped between a data transfer source and a data transfer destination.
[Means for Solving the Problems]
[0026]

The present invention is provided in considerations
25 of the above problems and relates to a data communication system that is adapted to transfer data between data communication apparatuses each having a memory adapted to store the data, and comprises communication means which transfers data contained in the memory of a first data
30 communication apparatus serving as a data transfer source to the memory of a second data communication apparatus

serving as a data transfer destination, state setting means which sets, in a stage in the course of data transfer processing with the communication means, states in the memory of each of the first and the second data communication apparatuses respectively in relation to a data entity serving as a transfer target, and memory access control means which brings into unauthorized, access to the data entity in the memory of at least one data communication apparatus when setting of a state representing a presence of the data entity serving as the transfer target in the memory of each of the first and the second data communication apparatuses is given.

[0027]

Provided that "the system" specified herein is referred to as a logically aggregate of more than one apparatus (or one functional module for implementing a specific function), and it does not matter whether or not each apparatus or functional module is contained in a single casing.

[0028]

The data communication system according to the present invention is of a type of data communication system adapted to transfer encrypted data through the contactless interface used in the IC card, for instance.

[0029]

As described above, the IC card (or the IC chip-mounted apparatus) is used as the place of safety to store the value information such as the electronic money and the electronic ticket or highly realizable digital data that is valuable as much as the cash.

[0030]

Now, with considerations of the convenience for the user, it is necessary to transfer the data contained in the IC card, in which case, however, as one adverse effect of an abnormal termination of the data transfer, there is a possibility of causing the data to be overlapped such that the data will remain in both of the data transfer source and the data transfer destination. In this case, the value information provider is obliged to provide the service beyond one's actually issued service, or the overlapped service, resulting in the detriment to one's interests.

[0031]

To the contrary, according to the present invention, in the stage in the course of the data transfer processing, the access to the data entity in the memory of at least one data communication apparatus is required to be placed into an unauthorized state in the presence of the data entity serving as the transfer target in both of the first data communication apparatus serving as the data transfer source and the second data communication apparatus serving as the data transfer destination.

[0032]

Thus, even in the presence of the data in both of the data communication apparatuses serving as the data transfer source and the data transfer destination, the data may be substantially prevented from being overlapped.

[0033]

In the present invention requires, each data communication apparatus serving as the data transfer source or the data transfer destination effects management of the data respectively held in its memory

after placing a data field adapted to hold the data into one of states including a valid state in which the access to the data contained in the data field is authorized, a state in which provisional creation of the data contained
5 in the data field is in process, a state in which the data contained in the data field is invalid, and a state in which deletion of the data from the data field is done. Then, the data field in each of the provisional creation and the invalid states results in the presence of the
10 data entity serving as the transfer target in the memory of each of the data communication apparatuses serving as the data transfer source and the data transfer destination, so that the data is prevented from being overlapped by prohibiting the access to the concerned
15 data entity in the memory of at least one data communication apparatus.

[0034]

In response to a data transfer instruction from the data communication apparatus serving as the data transfer
20 source, the data communication apparatus serving as the data transfer destination holds, in its memory, the data entity serving as the transfer target in the provisional creation state.

[0035]

25 Then, the data communication apparatus serving as the data transfer source, when receiving a transfer instruction response to the data transfer instruction from the data communication apparatus serving as the data transfer destination, places the held data in its memory
30 into the invalid state.

[0036]

Subsequently, the data communication apparatus serving as the data transfer source transmits a transfer acknowledgement instruction describing that the data serving as the transfer target was placed into the
5 invalid state. Then, in response to the transfer acknowledgement instruction, the data communication apparatus serving as the data transfer destination validates the held data in its memory in the provisional creation state.

10 [0037]

Then, the data communication apparatus serving as the data transfer destination gives a transfer acknowledgement response describing that its held data was placed into the valid state. In return for this, the
15 data communication apparatus serving as the data transfer source deletes the data in the invalid state from its memory in response to the transfer acknowledgement response.

[Effects of the Invention]

20 [0038]

According to the present invention, there may be provided the data communication system, the data communication method and the data communication apparatus that are excellent and adaptable to effect the data
25 communication between the data communication apparatuses adapted to transmit the encrypted data through the contactless interfaces.

[0039]

According to the present invention, there may be
30 also provided the data communication system, the data communication method and the data communication apparatus

that are excellent and adaptable to suitably transfer the value information such as the electronic money and the electronic ticket between the data communication apparatuses having the contactless interfaces.

5 [0040]

According to the present invention, there may be further provided the data communication system, the data communication method and the data communication apparatus that are excellent and adaptable to transfer the data
10 between the data communication apparatuses having the contactless interfaces while preventing the data from being overlapped between the data transfer source and the data transfer destination.

[0041]

15 The above and other objects, features and advantages of the present invention will become more apparent from the following detailed description of the presently preferred exemplary embodiment of the invention taken in conjunction with the accompanying drawing.

20 [Brief Description of the Drawings]

[FIG. 1]

FIG. 1 is a view schematically showing a configuration of a contactless IC card communication system to which the present invention is applicable.

25 [FIG. 2]

FIG. 2 is a view showing one configuration of a card reader/writer 1.

[FIG. 3]

FIG. 3 is a view showing one configuration of an IC
30 card 2.

[FIG. 4]

FIG. 4 is a view schematically showing a control system configuration of a memory area in the IC card according to the present invention.

[FIG. 5]

- 5 FIG. 5 is a view schematically showing an intra-IC card data structure serving as a transfer target in the present invention.

[FIG. 6]

- 10 FIG. 6 shows a sequence representing an operational procedure adapted to transfer data from one IC card to the other IC card using a contactless interface in the IC card.

[Explanation of reference numerals]

[0043]

- | | |
|----|----------------------------------|
| 15 | 1 ... Card reader/writer |
| | 2 ... IC card |
| | 3 ... Controller |
| | 21 ... IC chip module |
| | 23 ... Modulation circuit |
| 20 | 25 ... Demodulation circuit |
| | 27 ... Antenna |
| | 51 ... IC chip module |
| | 52 ... Capacitor |
| | 53 ... Antenna |
| 25 | 61 ... RF interface unit |
| | 62 ... BPSK demodulation circuit |
| | 63 ... PLL unit |
| | 64 ... Operating unit |
| | 65 ... ROM |
| 30 | 66 ... EEPROM |
| | 67 ... RAM |

- 68 ... BPSK modulation circuit
- 81 ... ASK demodulating unit
- 82 ... Voltage regulator
- 83 ... Oscillation circuit
- 5 84 ... ASK modulating unit
- 91 ... Sequencer
- 92 ... Encrypting/decrypting unit
- 93 ... Parity operating unit

[Best Mode for Carrying out the Invention]

10 [0044]

An embodiment of the present invention is now described in detail with reference to the accompanying drawings.

[0045]

15 Referring to FIG. 1, there is schematically shown a configuration of a contactless IC card communication system to which the present invention is applicable.

[0046]

20 This contactless card system is composed of a card reader/writer 1, an IC card 2, and a controller 3, and permits data to be transmitted and received between the card reader/writer 1 and the IC card 2 in a contactless manner by making use of electromagnetic waves.

Specifically, the card reader/writer 1 transmits a
25 prescribed command to the IC card 2, causing the IC card 2 to perform processing corresponding to the received command. Then, the IC card 2 transmits, to the card reader/writer 1, response data corresponding to a result of the above processing.

30 [0047]

The card reader/writer 1 is connected to the

controller 3 through a prescribed interface (an interface that conforms to RS-485A standards etc., for instance). The controller 3 supplies a control signal to the card reader/writer 1, causing prescribed processing to be put
5 into execution.

[0048]

Referring to FIG. 2, there is shown one configuration of the card reader/writer 1 shown in FIG. 1.

[0049]

10 An IC chip module 21 is configured with a DPU (Data Processing Unit) 31 to effect processing of the data, an SPU (Signal Processing Unit) 32 to effect processing of signals transmitted to and received from the IC card 2, an SCC (Serial Communication Controller) 33 to effect
15 communication with the controller 3, and a memory unit 34 including a ROM unit 41 preliminarily containing information required for data processing, and a RAM unit 42 to temporarily store partially completed work data, and these functional modules are interconnected through a
20 bus. Further, a flash memory 22 to store prescribed data is also connected to the bus.

[0050]

The DPU 31 outputs, to the SPU 32, a command to be transmitted to the IC card 2, and also receives the
25 response data from the IC card 2 through the SPU 32 to give prescribed data processing.

[0051]

The SPU 32 gives modulation processing such as BPSK (BiPhase Shift keying) to the command to be transmitted
30 to the IC card 2, before outputting to a modulation circuit 23, and also receives the response data from the

IC card 2 through a demodulation circuit 25 to give prescribed demodulation processing such as the BPSK to the received response data.

[0052]

5 The modulation circuit 23 ASK (Amplitude Shift Keying)-modulates a supplied carrier wave of a prescribed frequency (or 13.56 MHz, for instance) from an oscillator 26 with the supplied data from the SPU 32, causing a resultant modulated wave to be outputted as the
10 electromagnetic wave to the IC card 2 through an antenna 27. At this time, the modulation circuit 23 is required to set a modulation degree at less than 1 for ASK modulation. In other words, the maximum amplitude of the modulated wave needs to be provided without reaching zero,
15 even when the data is available at a low level.

[0053]

 The demodulation circuit 25 is configured to demodulate the modulated wave (or an ASK-modulated wave) having been received through the antenna 27, causing the
20 demodulated data to be outputted to the SPU 32.

[0054]

 Fig. 3 shows one configuration of the IC card 2 shown in FIG. 1. This IC card is composed of an IC chip module 51 and an antenna 53 on a loop.

25 [0055]

 The IC chip module 51 receives the modulated wave from the card reader/writer 1 through the antenna 53. It is to be noted that a capacitor 52 is combined with the antenna 53 to form a LC circuit so as to provide tuning
30 (or resonance) to the electromagnetic wave of a prescribed frequency (or a carrier frequency).

[0056]

The IC chip module 51 is composed of an RF interface unit 61 and an operating unit 64 etc. The RF interface unit 61 is composed of an ASK demodulating unit 81, a voltage regulator 82, an oscillation circuit 83, and an ASK modulating unit 84. The ASK demodulating unit 81 detects and demodulates the modulated wave (or the ASK-modulated wave) having been received through the antenna 53, causing the demodulated data to be outputted to a BPSK demodulation circuit 62 and a PLL (Phase Locked Loop) unit 63. The voltage regulator 82 stabilizes a signal having been detected by the ASK demodulating unit 81, before supplying as DC power to each circuit.

[0057]

The RF interface unit 61 also permits a signal of the same frequency as a data clock frequency to be oscillated with the oscillation circuit 83, causing the resultant signal to be outputted to the PLL unit 63. Then, the ASK modulating unit 84 ASK-modulates the modulated wave being received through the antenna 53 by fluctuating a load of the antenna 53 serving as a power supply of the IC card 2 (or by on-off controlling a prescribed switching element in correspondence to the data to connect a prescribed load to the antenna 53 in parallel only when the switching element is in an on state) in correspondence to the supplied data from the operating unit 84, causing a modulated component of the modulated wave to be transmitted to the card reader/writer 1 through the antenna 53. Whenever the transmission of the data from the IC card 2 takes place, the card reader/writer 1 provides the fixed maximum

amplitude of the modulated wave outputted therefrom, and accordingly, this modulated wave is ASK-modulated depending on a load fluctuation of the antenna 53. Further, with the above transmission of the data, a
5 terminal voltage in the antenna 27 of the card reader/writer 1 fluctuates.

[0058]

The PLL unit 63 generates, from the supplied data from the ASK demodulating unit 81, a clock signal
10 synchronized with the supplied data, causing the resultant clock signal to be outputted to the BPSK demodulation circuit 62 and the BPSK modulation circuit 68.

[0059]

15 In a case where the demodulated data produced by the ASK demodulating unit 81 is in the form of BPSK-modulated data, the BPSK demodulation circuit 62 effects the demodulation of the above modulated data according to the supplied clock signal from the PLL unit 63, causing
20 the demodulated data to be outputted to the operating unit 64.

[0060]

In a case where the supplied data from the BPSK demodulation circuit 62 is in the form of encrypted data,
25 after decrypting the encrypted data with an encrypting/decrypting unit 92, the operating unit 64 processes the data with a sequencer 91. Conversely, in a case of the data obtained without being encrypted, the supplied data from the BPSK demodulation circuit is
30 directly supplied to the sequencer 91 without passing through the encrypting/decrypting unit 92.

[0061]

The sequencer 91 performs the processing corresponding to the data serving as the command supplied to the sequencer. For instance, the sequencer 91 is
5 adapted to perform the processing such as write and readout of data with respect to an EEPROM (Electrically Erasable & Programmable ROM) 66.

[0062]

A parity operation unit 93 of the operating unit 64
10 calculates a read Solomon code as parity from the data stored in and/or contained in the EEPROM 66. Further, after giving prescribed processing with the sequencer 91, the operating unit 64 outputs, to the BPSK modulation circuit 68, the response data (or the data to be
15 transmitted to the card reader/writer 1) corresponding to the above processing.

[0063]

The BPSK modulation circuit 68 BPSK-modulates the supplied data from the operating unit 64, causing the
20 modulated data to be outputted to the ASK modulating unit 84 of the RF interface unit 61.

[0064]

The ROM 65 permanently contains a processing program that the sequencer 91 executes and other required
25 data. The RAM 67 is to temporarily store work data etc. that is used at the time when the sequencer 91 performs the processing.

[0065]

The EEPROM 66 is a nonvolatile memory, and is used
30 to store, on the IC card 2, a large number of applications such as the electronic money for the

electronic payment and the electronic ticket for the admission to a specific concert hall. The IC card 2 itself basically has no drive power supply such as a battery, so that it is necessary to use the non-volatile
5 memory like the EEPROM 66 that may keep hold of the data also in a power off state even after a termination of the communication with the card reader/writer 1 by the IC card 2 brings a feed of power to a stop.

[0066]

10 Processing for data transmission and reception between the card reader/writer 1 and the IC card 2 is now described.

[0067]

The card reader/writer 1 stands ready until a load
15 state change with access of the IC card 2 is detected, while monitoring a load state of the antenna 27 by radiating a prescribed electromagnetic wave through the antenna 27. It is noted that the card reader/writer 1 may be also configured to take some processing (or
20 polling) for repeatedly effecting the polling to the IC card 2 until a response from the IC card 2 is acknowledged within a certain period of time by radiating the ASK-modulated electromagnetic wave produced with data of a relatively short pattern.

25 [0068]

If the access of the IC card 2 is detected in the card reader/writer 1, the SPU 32 of the R/W 1 effects the BPSK modulation with the data (such as the command
30 corresponding to the processing to be performed by the IC card 2 and the data to be written on the IC card 2) to be transmitted to the IC card 2 using a rectangular wave of

a prescribed frequency (or a frequency twice as large as the data clock frequency) as the carrier wave, causing the resultant modulated wave (or a BPSK-modulated signal) to be outputted to the modulation circuit 23.

5 [0069]

It is noted that on the occasion of the BPSK modulation, use of a differential conversion permits the data to be adapted to meet a phase change of the modulated wave. In such a case, even if an inversion of the BPSK-modulated signal occurs, the demodulation into its original data is executable, thereby eliminating any need to take account of a modulated wave polarity at the time of the demodulation.

[0070]

15 The modulation circuit 23 ASK-modulates the prescribed carrier wave with the supplied BPSK-modulated signal at the modulation degree (= the maximum amplitude of the data signal/the maximum amplitude of the carrier wave) of less than 1 (0.1, for instance), causing the resultant modulated wave (the ASK-modulated wave) to be transmitted to the IC card 2 through the antenna 27.

[0071]

It is noted that when no transmission is performed, the modulation circuit 23 generates the modulated wave at one of two levels (high and low levels) of a digital signal or the high level, for instance.

[0072]

The IC card 2 permits, in an LC circuit composed of the antenna 53 and the capacitor 52, a part of the radiated electromagnetic wave from the card reader/writer 30 1 through the antenna 27 to be converted into an electric

signal, causing the resultant electric signal (or the modulated wave) to be outputted to the RF interface 61 of the IC chip module 51. Then, the ASK demodulating unit 81 of the RF interface 61 effects envelop detection by smoothing the modulated wave through rectification, causing the resultant signal to be supplied to the voltage regulator 82, and also extracts a data signal by suppressing a DC component of the above signal, causing the extracted data signal to be outputted to the BPSK demodulation circuit 62 and the PLL unit 63.

[0073]

The voltage regulator 82 stabilizes the supplied signal from the ASK demodulating unit 81 to generate the DC power, and supplies the resultant power to each circuit.

[0074]

It is noted that a terminal voltage V_0 of the antenna 53 at this time is expressed as follows, for instance.

[0075]

$$V_0 = V_{10}(1 + k \times V_s(t))\cos(\omega t)$$

[0076]

Wherein $V_{10}\cos(\omega t)$ represents the carrier wave, k is the modulation degree, and $V_s(t)$ is data outputted from the SPU 32, respectively.

[0077]

Further, a low-level value V_{LR} in a voltage V_1 obtained after rectification by the ASK demodulating unit 81 is expressed as follows, for instance.

[0078]

$$V_{LR} = V_{10} (1 + k \times (-1)) - V_f$$

[0079]

Wherein V_f represents a voltage fall in a diode contained in a rectification circuit adapted to effect smoothing through rectification in the ASK demodulating unit 81, and is generally as much as about 0.7 volts.

[0080]

The voltage regulator 82, when receiving the signal having been given the smoothing through rectification by the ASK demodulating unit 81, stabilizes the received signal, before supplying as the DC power to each circuit including the operating unit 64. It is noted that the modulation degree k of the modulated wave is less than 1, so that a rectified voltage fluctuation (a difference between the high and the low levels) is small. Thus, in the voltage regulator 82, a generation of the DC power is easily attainable.

[0081]

For instance, in a case where the modulated wave with the modulation degree k of 5% is received so as to have V_{10} of 3 volts or above, the rectified low-level voltage V_{LH} results in 2.15 ($= 3 \times (1 - 0.05) - 0.7$) volts or above, permitting the voltage regulator 82 to supply an adequate voltage as the power supply to each circuit. In this case, the amplitude $2 \times k \times V_{10}$ (Peak-to-Peak value) of an AC component (or a data component) of the rectified voltage V_1 results in 0.3 ($= 20.05 \times 3$) volts or above, permitting the ASK demodulating unit 81 to demodulate the data at a sufficiently high S/N ratio.

[0082]

As described above, use of the ASK-modulated wave with the modulation degree k of less than 1 provides the

communication ensuring a low error rate (in a state of a high S/N ratio), and also permits the adequate DC voltage as the power supply to be supplied to the IC card 2.

[0083]

- 5 The BPSK demodulation circuit 62, when receiving the data signal (the BPSK-modulated signal) from the ASK demodulating unit 81, demodulates the received data signal according to the supplied clock signal from the PLL unit 63, and outputs the demodulated data to the
10 operating unit 64.

[0084]

- In a case where the supplied data from the BPSK demodulation circuit 62 is in the form of the encrypted data, after decrypting the data with the
15 encrypting/decrypting unit 92, the operating unit 64 supplies the data (the command) to the sequencer 91 for processing of the data. It is noted that for a period between the transmission of the data to the IC card 2 and the reception of the response to the transmitted data,
20 the card reader/writer 1 stands ready as it is after having transmitted the data assigned a value of 1. Thus, in the above period, the IC card 2 receives the modulated wave having the fixed maximum amplitude.

[0085]

- 25 After a completion of the processing, the sequencer 91 outputs, to the BPSK modulation circuit 68, the data to be transmitted to the card reader/writer 1. Like the SPU 32 at the card reader/writer 1-side, after BPSK-modulating the supplied data, the BPSK modulation circuit
30 68 outputs the data to the ASK modulating unit 84 of the RF interface unit 61.

[0086]

The ASK modulating unit 84 may apply the switching element to fluctuate loads connected to the opposite ends of the antenna 53. Specifically, the load variation
5 caused depending on the data from the BPSK modulation circuit 68 is adapted to ASK-modulate the received modulated wave depending on the data to be transmitted, thereby causing the terminal voltage of the antenna 27 of the card reader/writer 1 to be fluctuated before the
10 transmission of the data to the card reader/writer 1.

[0087]

On the other hand, the modulation circuit 23 at the card reader/writer 1-side keeps up the transmission of the data assigned the value of 1 (the high level) at the
15 time of the reception of the data from the IC card 2. Then, in the demodulation circuit 25, the data having been transmitted from the IC card 2 is detected based on a minute fluctuation (several ten micro-volts, for instance) of the terminal voltage of the antenna 27
20 electromagnetic-coupled with the antenna 53 of the IC card 2.

[0088]

Further, the demodulation circuit 25 permits the detected signal (the ASK-modulated wave) to be modulated
25 after being amplified with a high gain amplifier, and outputs the resultant digital data to the SPU 32. The SPU 32 demodulates the received digital data (the BPSK-modulated signal), and outputs the data to the DPU 31. The DPU 31 processes the data from the SPU 32, and judges
30 depending on the result of processing whether or not the communication is to be terminated.

[0089]

Then, in a case where it is determined that the communication is to be performed again, the communication between the card reader/writer 1 and the IC card 2 is
5 effected in the same manner as the above case.

Conversely, in a case where it is determined that the communication is to be terminated, the card reader/writer 1 terminates the processing for the communication with the IC card 2.

10 [0090]

As described above, the card reader/writer 1 transmits the data to the IC card 2 by making use of the ASK modulation with the modulating factor k of less than 1. Then, the IC card 2 receives the above data to
15 perform the processing corresponding to the received data, and transmits the data corresponding to the result of the processing back to the card reader/writer 1.

[0091]

Referring to FIG. 4, there is schematically shown a
20 configuration of a memory area control system in the IC card according to the embodiment of the present invention. As shown in FIG. 4, this control system is basically implemented as a subsystem contained in an operating system, and is composed of a protocol interface unit, an
25 OS core unit, and a file system.

[0092]

The protocol interface unit handles a request for external apparatus access to the file system through an external apparatus interface such as UART, or a request
30 for card read/write apparatus access to the file system through the contactless IC card interface.

[0093]

The OS core unit is adapted to perform the processing such as decoding/encoding of data exchanged with the file system, error correction with a CRC etc.,
5 checking of the number of rewrite times for each block of the EEPROM 66, PIN matching and mutual authentication etc.

[0094]

Further, the OS core unit is equipped with some APIs (Application Programming Interfaces) to the file
10 system for the processing such as the PIN matching and the mutual authentication both required at the time of file access and file read/write etc.

[0095]

The file system provides physical access to the
15 EEPROM 66 serving as a file system entity. An action itself of the physical access to a memory device such as the EEPROM is well known to those skilled in the concerned industry, so that description thereof is omitted here.

20 [0096]

The memory area expanded on an EEPROM 43 is composed of one or more file systems. In an initial state, the memory area is managed by a single file system under control of an original IC card issuer. When a
25 service source provider other than the IC card issuer attempts to divide a new file system from the memory area, a memory area division authorization and an authentication to the original IC card issuer are both required. Once divided, the authentication that is not
30 to the original IC card issuer but to the service source provider of the file system itself is required for the

access to the file system. To divide the file system is the same as to issue a virtual IC card.

[0097]

The OS manages a division authorization key K_d for
5 giving an authorization to divide the memory area.
Further, an issuer key k_i for the issuer (the original IC
card issuer or a provider having an experience in
dividing the file), a system code and an area ID for file
area identification are also under management for each
10 file system.

[0098]

The access to the file system is made through steps
including an area ID request by polling and the mutual
authentication. A file system issuer (the card issuer in
15 the case of the original file system or the service
source provider using the divided file system) may
acquire the area ID available on the memory area of the
concerned file system by, at first, effecting the polling
to the file system with its appreciated system code as an
20 argument. Next, the mutual authentication is followed
using the acquired area ID and the issuer key K_i . Then,
when the mutual authentication results in success, the
access to the file system is permitted. The access to
the file system requires encrypted communication
25 involving use of the issuer key K_i unique to the file
system relevant to the issuer, resulting in no
authorization to capture irrelevant data by the other
file system, or to perform reading and writing with
respect to the file system by those other than the issuer
30 without permission.

[0099]

Processing for the data transfer involving use of the contactless interface in the IC card is now described.
[0100]

The data transfer specified herein includes not
5 only the IC card-to-IC card transfer but also the transfer of data from the IC card to the IC chip-mounted apparatus (such as the mobile phone and the other types of mobile apparatuses) and the transfer of data from one IC chip-mounted apparatus to the other. For the sake of
10 convenience, the IC card and the IC chip-mounted apparatus are hereinafter altogether referred to as the IC card. Further, the data serving as the transfer target is not limited to data in the whole memory area in the IC card and may be data in either expanded or divided
15 file system units available on the memory area or file (or service) units of a file system lower than a specific one. For the sake of convenience, it is simply referred to as "data".

[0101]

20 Unlike a radio LAN providing a relatively wide range of radio waves or a wired interface, in the contactless interface in the IC card, a connection state is maintained with the interfaces spaced at a relatively short distance, so that there are cases where some
25 unexpected accidents cause the contactless interface to be pulled apart, resulting in the cut of the connection, or alternatively, the contactless communication results in no normal termination by other causes.

[0102]

30 As one adverse effect of an abnormal termination of the data transfer, there is one problem of causing the

data to be overlapped such that the data will remain in both of the data transfer source and the data transfer destination.

[0103]

5 The IC card (or the IC chip-mounted apparatus) is used as the place of safety to store the value information such as the electronic money and the electronic ticket, that is, the highly realizable digital data that is valuable as much as the cash. If
10 overlapping of the data occurs, the value information provider is obliged to provide the service beyond one's actually issued service or the overlapped service, resulting in the detriment to the value information provider.

15 [0104]

To the contrary, the contactless data communication according to the embodiment of the present invention is adaptable to completely prevent the data in the process of being transferred from being overlapped even when a
20 processing break occurs in any stage in the course of the data transfer, as described in the following.

[0105]

The embodiment of the present invention requires that the data (that is, the data serving as the transfer
25 target) stored in the IC card is composed of a data field to write actual data and a state field to record a state of the data contained in the data field, as shown in FIG. 5.

[0106]

30 Four types of states, "valid", "provisional creation", "invalid" and "delete", are defined as data

field states for the period of the data transfer between the IC cards. Then, a current state of the data field needs to be written in the state field.

[0107]

5 The valid state means a state in which the data field of the IC card is validly available. Thus, the operating system of the IC card may provide access, through prescribed authentication processing, to a request for external access to the data field containing
10 a description to the effect of valid in the data field or to the file system.

[0108]

15 The provisional creation state means a state in which in the course of the data transfer between the IC cards, creation of a valid data field serving as the transfer target in the memory area of the IC card serving as the transfer destination is in process. Although the data field in the provisional creation state is available with the valid data entity contained, no validity exists
20 as the state of the concerned field. Thus, the operating system of the IC card denies the request for access to the data field containing the description to the effect of provisional creation in the state field or to the file system.

25 [0109]

30 The invalid state means a state in which in the course of the data transfer between the IC cards, the original data left behind in the memory area of the IC card as the transfer source is invalid or ought not to be used any more, because of a completion of the generation of the provisional creation data field serving as the

transfer target in the memory area of the IC card serving as the transfer destination. Although the data field in the provisional creation state is available with the valid data entity contained, no validity exists as the state of the concerned field. Thus, the operating system of the IC card denies the request for access to the data field containing the description to the effect of invalid in the state field or to the file system.

[0110]

The delete state means a state in which in the course of the data transfer between the IC cards, the original data contained in the memory area of the IC card as the transfer source does not need to be preserved any more, after the provisional creation data field serving as the transfer target in the memory area of the IC card serving as the transfer destination has been validated. It is at the option to completely delete the data field placed into the delete state or give only the description indicating the delete state. The data field in the delete state is reusable for rewriting etc. after erasing. Thus, the operating system of the IC card takes an action of access to the data field through the predetermined authentication processing whenever external write access occurs.

[0111]

It is noted that each of the data fields in the provisional creation and the invalid states, although ensuring that the contained data entity itself is valid, is in the state where ordinary access through the contactless interface is prohibited. The termination in the data provisional creation state causes the data to be

placed into the invalid state in the IC card as the transfer source, and also into the provisional creation state in the IC card as the transfer destination as described later, in which case, use of the data with
5 either the card becomes unauthorized, resulting in creation of the same state as a data lost state. In such a case, it is also allowable to provide a service for recovery of the data field from the invalid or provisional creation state to the valid state through
10 operations by a card administrator.

[0112]

An operation procedure for the data transfer from one IC card to the other IC card using the contactless interfaces in the IC cards is now described with
15 reference to FIG. 6. Provided that in FIG. 6, with a data transfer source apparatus specified as an IC card A, a data transfer destination apparatus is specified as an IC card B. Further, with an encrypted data transmission line established between the IC cards A and B with the
20 contactless interfaces through a prescribed authentication procedure, each communication step shown in the following requires that the communication is effected using this transmission line.

[0113]

25 Step 1)

A data transfer instruction is transmitted from the IC card A to the IC card B. A data transfer instruction message frame is formed of a combination of a transfer instruction command and a data entity serving as the
30 transfer target.

[0114]

Step 2)

The IC card B, when receiving a transfer instruction message, effects provisional creation of the data. Specifically, after writing of the data entity
5 contained in the message onto its memory area, the state of the data field is placed into "provisional creation". Further, an IC card A's ID contained in the transfer instruction is assigned to the provisional creation data.
[0115]

10 At this stage, the data entity serving as the transfer target is present in both of the IC cards A and B. Although the data field in the provisional creation state is available with the valid data entity contained, no validity exists as the state of the concerned field.
15 Thus, the operating system of the IC card B rejects the request for access to the data field containing the description to the effect of provisional creation in the state field or to the file system. In other words, the data is substantially prevented from being overlapped.
20 [0116]

Then, the IC card B transmits, back to the IC card A, a transfer instruction response message describing an acknowledgement of the transfer instruction involved in the step 1).

25 [0117]

Step 3)

The IC card A receives the transfer instruction response message from the IC card B, causing the state of the transmitted data field in the step 1) to be invalid.
30 An IC card B's ID contained in the transfer instruction response is assigned to the invalidated data data field.

[0118]

At this stage, the data entity serving as the transfer target is present in both of the IC cards A and B. Although the valid data entity is described in the data field in the invalid state, no validity exists as the state of the concerned field. Thus, the operating system of the IC card A rejects the request for access to the data field containing the description to the effect of invalid in the state field or to the file system. In other words, the data is substantially prevented from being overlapped.

[0119]

Then, the IC card A transmits, back to the IC card B, a transfer acknowledgement instruction message serving as an acknowledgement to the transfer instruction response involved in the Step 2).

[0120]

Step 4)

After the reception of the response or the transfer acknowledgement message involved in the step 3), the IC card B transforms the provisional creation data into actual data. Specifically, the state of the data field containing the received data in the step 2) is updated so as to change from "provisional creation" to "valid".

[0121]

The valid state means the state in which the data field of the IC card is authorized to be validly available. Thus, the operating system of the IC card B may provide access, through the prescribed authentication processing, to the request for external access to the data field containing the description to the effect of

valid in the state field or to the file system.

[0122]

Further, while at this stage, the data entity serving as the transfer target is present in both of the
5 IC cards A and B, the IC card A-side is available with the data field placed into the invalid state, so that the data is substantially prevented from being overlapped.

[0123]

Further, the IC card B transmits, back to the IC
10 card A, a transfer acknowledgement response message serving as the response to the transfer acknowledgement instruction.

[0124]

Step 5)

15 The IC card A, when receiving the transfer acknowledgement response message, deletes the data from the invalidated data field. The data field in the delete state means that it is in the state where in the course of the data transfer between the IC cards, the original
20 data contained in the memory area of the IC card as the transfer source does not need to be preserved any more, after the provisional creation data field serving as the transfer target in the memory area of the IC card serving as the transfer destination has been validated. It is at
25 the option to completely delete the data field placed into the delete state or to give only the description to the effect of the existence of the delete state.

[0125]

At a stage of completion of the above data transfer
30 process, the data entity serving as the transfer target is found only in the IC card B, permitting the data to be

provided without being overlapped.

[0126]

It is desired to fully understand that use of the above steps 1) to 5) makes it possible to eliminate the presence of the overlapped data. However, a situation exists that the data is invalidated, so that it is necessary for this case to take means that allows the data issuer to check the situation and restore the data.

[0127]

It is noted that while the encrypted data transmission line preferably needs to be established between the IC cards A and B with the contactless interfaces in order to suitably implement the present invention, no limitation is particularly imposed on a form of the encrypted data transmission line.

[0128]

For instance, Japanese Patent Application Publication (KOKAI) 2002-24778 having been already assigned to the present applicant provides a disclosure on a data communication method in which with a reader/writer held in close contact together with the same type of IC cards, coupling with integrated antennas of the same type of IC cards through a reader/writer antenna is adapted to directly exchange the data between the same type of IC cards, permitting copy of records to be effected between built-in memories of the same type of IC cards. Accordingly, it is also allowable to apply the above data communication method to transfer the data between the IC cards A and B.

[Industrial Applicability]

[0129]

The present invention has been heretofore described in detail with reference to the specific embodiment. However, it is obvious to those skilled in the art that various modifications and substitutions of the above
5 embodiment may be made without departing from the scope of the present invention.

[0130]

While the present specification has described in relation to the configuration of the present invention
10 together with its operations and effects, mainly to the embodiment available for the application of the present invention to the data communication system involving use of the encrypted data transmission line established with the contactless interfaces used in the IC cards, the
15 scope of the present invention is not limited to the above. In other words, the present invention, even when applied to cases involving use of any type of communication interface, is adaptable to suitably prevent the data from being overlapped between the data transfer
20 source apparatus and the data transfer destination apparatus in the process of the data transfer.

[0131]

In conclusion, the disclosure of the present invention has been given in the form of illustrations,
25 and the contents of the present specification are therefore illustrative and not restrictive. The scope of the present invention is to be determined in considerations of the description of claims.

CLAIMS

1. A data communication system for transferring data between data communication apparatuses having memories adapted to store data, characterized by having:

communication means which transfers the data stored in a memory of a first data communication apparatus serving as a data transfer source to a memory of a second data communication apparatus serving as a data transfer destination;

state setting means which respectively sets, in a stage in the course of data transfer processing with said communication means, states in a memory of each of said first and said second communication apparatuses in relation to a data entity serving as a transfer target; and

memory access control means which brings, into unauthorized, access to said data entity in the memory of at least one data communication apparatus, in a case where a state representing a presence of the data entity serving as the transfer target in the memory of each of said first and said second communication apparatuses is set.

2. The data communication system according to claim 1, characterized in that:

said communication means effects transfer of the data between the memories of said first and said second communication apparatus through data communication involving use of an encrypted data transmission line established with contactless interfaces.

3. The data communication system according to claim 1, characterized in that:

said state setting means places a data field
5 adapted to hold the data entity in the memory of each of
said first and said second data communication apparatuses
into one of states including a valid state in which
access to the data contained in the data field is
authorized, a state in which provisional creation of the
10 data contained in the data field is in process, a state
in which the data contained in the data field is invalid,
and a state in which the data is deleted from the data
field, and

said memory access control means prohibits the
15 access to the data field placed into the provisional and
invalid states in the memory of each of said first and
said second data communication apparatuses.

4. The data communication system according to claim 3,
20 characterized in that:

in response to that a data transfer instruction was
issued from said first data communication apparatus, said
state setting means places, into the provisional creation
state, the held data entity as the transfer target in the
25 memory of said second data communication apparatus.

5. The data communication system according to claim 4,
characterized in that:

in response to that a transfer instruction response
30 to said data transfer instruction was transmitted from
said second data communication apparatus, said state

setting means places, into the invalid state, the held data entity in the memory of said first data communication apparatus.

- 5 6. The data communication system according to claim 5, characterized in that:

in response to that said first data communication apparatus transmitted a transfer acknowledgement instruction describing that the data entity serving as
10 the transfer target was placed into the invalid state, said state setting means places, into the valid state, the held data entity in the provisional creation state in the memory of said second data communication apparatus.

- 15 7. The data communication system according to claim 6, characterized in that:

in response to that said second data communication apparatus transmitted a transfer acknowledgement response describing that the held data entity in the memory was
20 placed into the valid state, said state setting means deletes the held data entity in the invalid state from the memory of said first data communication apparatus.

8. A data communication method of transferring data
25 between data communication apparatuses having memories adapted to store data, characterized by having:

a step in which, in response to a data transfer instruction from a first data communication apparatus serving as a data transfer source, a second data
30 communication apparatus serving as a data transfer destination places data serving as a transfer target into

a provisional creation state, before holding said data in its memory;

a step in which said first data communication apparatus receives a transfer instruction response to the
 5 data transfer instruction from said second data communication apparatus and places the held data in its memory into an invalid state;

a step in which said first data communication apparatus transmits a transfer acknowledgement
 10 instruction describing that the data serving as the transfer target was placed into the invalid state;

a step in which, in response to said transfer acknowledgement instruction, said second data communication apparatus validates the held data in the
 15 provisional creation state in its memory;

a step in which said second data communication apparatus transmits a transfer acknowledgement response describing that the held data in its memory was placed into the valid state; and

20 a step in which, in response to said transfer acknowledgement response, said first data communication apparatus deletes the held data in the invalid state from its memory; and characterized in that:

access to the data field placed into the
 25 provisional creation or invalid state in the memory of each of said data communication apparatuses is prohibited.

9. A data communication apparatus for transferring data, characterized by having:

30 data communication means which effects communication of data;

communication control means which controls a data communication operation;

data holding means which holds the data; and

data management means which manages the data

5 contained in said data holding means, and

characterized in that:

said data management means places a data field adapted to hold the data into one of states including a valid state in which access to the data contained in the data field is authorized, a state in which provisional
10 creation of the data contained in the data field is in process, a state in which the data contained in the data field is invalid, and a state in which the data is deleted from the data field, causing the access to the
15 data field in the provisional creation and invalid states to be prohibited.

10. The data communication apparatus according to claim 9, characterized in that:

20 said data communication means effects data communication involving use of an encrypted data communication line established with contactless interfaces.

25 11. The data communication apparatus according to claim 9, characterized in that:

in a case of operating as a data transfer source apparatus,

said communication control means issues a
30 transfer instruction to a data transfer destination apparatus, and also a transfer acknowledgement.

instruction to a transfer instruction response from the data transfer destination apparatus, and

5 said data management means, when receiving the transfer instruction response, invalidates the data serving as the transfer target, and when receiving a transfer acknowledgement response to the transfer acknowledgement instruction, deletes the invalidated data.

12. The data communication apparatus according to claim 10 9, characterized in that:

in a case of operating as the data transfer destination apparatus,

15 said communication control means transmits a transfer instruction response in response to the transfer instruction from the data transfer source apparatus, and also a transfer acknowledgement response in response to the transfer acknowledgement instruction, and

20 said data management means effects provisional creation of the data serving as the transfer target after being received together with the transfer instruction, and validates the provisional created data in response to the transfer acknowledgement instruction.