

DESCRIPTION

DATA COMMUNICATION APPARATUS AND METHOD FOR MANAGING MEMORY
OF DATA COMMUNICATION APPARATUS

Technical Field

[0001]

The present invention relates to a data communication apparatus including a relatively high-capacity memory and a method for managing the memory of the data communication apparatus and, in particular, to a data communication apparatus for storing electronic value information in a memory area and communicating secure information including electronic payment information and a method for managing the memory of the data communication apparatus.

[0002]

More specifically, the present invention relates to a data communication apparatus for allocating a file system for a service provider in a memory area and managing information about services provided by the service provider using the file system and a method for managing the memory of the data communication apparatus and, in particular, to a data communication apparatus for allocating a file system for each of a plurality of service providers in a single memory area and allowing the plurality of service providers to share the single data communication apparatus in order to

provide a plurality of services and a method for managing the memory of the data communication apparatus.

Background Art

[0003]

Examples of wireless communication means that is applicable only in a local area include a contactless IC card.

[0004]

In general, this type of wireless communication is realized on the basis of the principal of electromagnetic induction. That is, the wireless communication is performed by an IC card having a memory function and a card reader/writer for accessing a memory of the IC card to read information from and write information to the memory. A loop coil of the IC card serves as a primary coil and an antenna of the card reader/writer serves as a secondary coil so as to form a transformer as a system. The card reader/writer transmits electric power and information to the IC card using electromagnetic induction. The IC card can operate using the supplied electric power so as to respond to an inquiry signal from the card reader/writer.

[0005]

When the card reader/writer modulates an electric current passing through the antenna, the induced voltage of the loop coil of the IC card is modulated. Using this

effect, the card reader/writer can transmit data to the IC card. Additionally, as the load between terminals of the loop coil of the IC card varies, the impedance between antenna terminals of the IC card reader/writer varies, and therefore, the passing electric current or the voltage of the antenna varies. Using this effect, the IC card can transmit a response to the card reader/writer.

[0006]

Contactless short-range communication systems including the IC card have been in widespread use due to the simplicity of operation. For example, a security code, other personal identification information, and electronic value information (e.g., an electronic ticket) are stored in the IC card. On the other hand, the card reader/writers are disposed in a cash dispenser, at the entrances/exits of a concert hall, and at a ticket gate of a railway station. When a user places the IC card above the card reader/writer, the IC card can contactlessly access the card reader/writer. Thus, the authentication process can be performed.

[0007]

Recently, with the improvement in fine processing technology, an IC card having a relatively high-capacity memory space has been realized. Since the IC card having a high-capacity memory can store a plurality of applications at the same time, the IC card can be used for a plurality of

purposes. For example, one IC card that stores a plurality of applications (e.g., electronic money and an electronic ticket for a specific concert hall) can be used for a variety of purposes. Here, the terms "electronic money" and "electronic ticket" refer to a payment (electronic payment) system using electronic data issued to a user in accordance with a fund provided by the user or such electronic data itself.

[0008]

In general, the IC card is used by a user placing the IC card above the card reader/writer. The card reader/writer poles an IC card at all times. When the card reader/writer finds an external IC card, the communication between the IC card and the card reader/writer starts.

[0009]

At that time, the user inputs the security code to the card reader/writer. The card reader/writer compares the input security code with the security code stored in the IC card. Thus, the personal identity verification or authentication process is performed between the IC card and the card reader/writer. This security code used during accessing the IC card is referred to as a "personal identification number (PIN)". If the personal identity verification or authentication process is successful, the user can use an application stored in the IC card, for

example. That is, the user can access a service memory area allocated to the application (hereinafter referred to as a "service memory area"). When accessing the service memory area, appropriate encrypted communication is performed depending on the security level of the application.

[0010]

Furthermore, if the IC card and the card reader/writer (card reader/writer apparatus) include a wired interface (not shown) for communicating with an external apparatus in addition to the wireless contactless interface, the function of either one of the IC card and the card reader/writer or both can be provided to an apparatus, such as a cell phone, a personal digital assistant (PDA), a consumer electronics (CE) apparatus, and a personal computer. In such a case, the IC card technology can be applied to a general bi-directional short range communication interface.

[0011]

For example, when the short range communication is performed among computers and home information appliances, one-to-one communication using the IC card is performed therebetween. In addition, some apparatus can communicate with an apparatus other than a contactless IC card. In such a case, an application can be provided in which one-to-many communication is performed between one apparatus and a plurality of cards.

[0012]

Additionally, a variety of applications that use an IC card in order to externally communicate electronic value information (such as electronic payment) can be run on an information processing apparatus. For example, by using a keyboard and a display on the information processing apparatus, a user can communicate with the IC card. Since the IC card is connected to a cell phone, a user can send information stored in the IC card via a telephone line. Furthermore, using the IC card, the user can send payment from the cell phone via the Internet.

[0013]

If a file system for a service provider is allocated in an internal memory of the IC card and service information used for the service provider (e.g., user identification/authentication information, information about the remaining value, or the use history (log)) is managed in the file system, a useful service based on contactless short-range communication that is the replacement for a known prepaid card and a service card provided by each store can be achieved.

[0014]

Conventionally, each service provider issues an IC card to a user to provide the service thereof. Accordingly, the user has a plurality of cards, each used for one service,

and carries the cards with them. In contrast, according to an IC card that has a relatively high-capacity memory space, the IC card can provide sufficient memory space for storing information about a plurality of services in the internal memory.

[0015]

For advance-payment-type cards, such as prepaid cards, to ensure proper business conduct for issuing the cards, protect the purchasers of the cards, and ensure the credibility of the cards, "A law regarding the regulation of the advance-payment-type cards and the like" (known as the "purika" law) has been established so that the issuers of advance-payment-type cards must register with the authorities and are regulated by the law. Also, according to the law, for providing a convenient service to users and maintaining marketing order, predetermined items, such as a logo and the contact address must be printed on a prepaid card (on a surface of the card) (see section 12 of the law).

[0016]

When providing a prepaid card that stores prepaid information in the memory thereof, the number of providing services is limited to one due to the printing of information on a medium regulated by the law. In contrast, when an IC card function is used on a mobile device (e.g., a cell phone) having a display function, the requirement of

the regulation of the law can be satisfied by displaying information related to the desired value information (refer to, for example, Patent Document 1). Thus, a plurality of service providers can share the IC card function.

Accordingly, for the service providers, the workload to issue a card is reduced whereas, for the users, the number of IC cards that the user should carry with them is reduced.

[0017]

Unfortunately, when a plurality of service providers share a single memory area and each service provider is allowed to freely access a memory area of a different service provider which shares the memory, the value information set for each service provider may be used by the different unauthorized service provider. As a result, the service provider cannot provide a reliable service. Also, the user has the risk of leakage of the value information with high liquidity, thus suffering economic loss.

[0018]

Therefore, in the case where a plurality of service providers share an IC card, it is required that the user can consider the IC card to be a card that each service provider originally issues when the user uses the service. In addition, the IC card is required to have a feature to securely manage the information for each service provider in the memory area.

[0019]

[Patent Document 1]

Japanese Unexamined Patent Application Publication No. 2003-141434

Disclosure of Invention

Problems to be Solved by the Invention

[0020]

The embodiments of present invention provide an excellent data communication apparatus and method for managing a memory of the data communication apparatus that can store electronic value information in the memory area and securely exchange the information for, for example, electronic payment.

[0021]

The embodiments of present invention further provide an excellent data communication apparatus and method for managing a memory of the data communication apparatus that can provide a user with ease of use as if an IC card were directly issued by a service provider of the service that the user is currently using and that has a mechanism to securely manage information about a plurality of service providers in a memory area so that the plurality of service providers can share one IC card.

[0022]

In a first aspect of the invention, there is provided a data communication apparatus having a memory space, the data communication apparatus managing the memory space by separating the memory space into one or more file systems, the apparatus comprising: controlling means for holding a separating authority key and managing the access to the file system in the memory space; and a first file system allocated to a first service provider in the memory space, the first file system holding an issuer key of the first service provider; wherein, upon receiving, from a second service

provider requesting an allocation of a new file system, a separate package generated by encrypting, using the issuer key of the first service provider, a data block containing a separate element package generated by encrypting an issuer key of the second service provider using the separating authority key and information on the new file system, the first file system decrypts the received separate package using the issuer key of the first service provider and retrieves the separate element package and the information on the new file system, and wherein the controlling means decrypts the separate element package using the separating authority key, retrieves the issuer key of the second service provider, separates a free area of the memory space in accordance with the information on the new file system, and allocates the separated memory area to a second file system holding the issuer key of the second service provider.

In a second aspect of the invention, there is provided a method for managing a memory of a data communication apparatus, the data communication apparatus having a memory space and managing the memory space by separating the memory space into one or more file systems, wherein a separating authority key for authenticating authority to separate the file system and a first file system for authenticating access authority using an issuer key of a first service provider are provided in the memory space, the method comprising the steps of: receiving, from a second service provider requesting an allocation of a new file system, a separate package generated by encrypting, using the issuer key of the first service

provider, a data block containing a separate element package generated by encrypting an issuer key of the second service provider using the separating authority key and information on the new file system; decrypting the received separate package using the issuer key of the first service provider and retrieving the separate element package and the information on the new file system; and decrypting the separate element package using the separating authority key, retrieving the issuer key of the second service provider, separating a free area of the memory space in accordance with the information on the new file system, and allocating the separated memory area to a second file system holding the issuer key of the second service provider. As used herein, the term "data communication apparatus" refers to a contactless IC card including a wireless communications unit and an IC chip having a data reception/transmission function and a data processing unit, a contact IC card having a terminal on the surface thereof, or an information communications apparatus (e.g., a cell phone, a personal handyphone system (PHS), or a personal digital assistance

(PDA)) including an IC chip having the same function as that of a contact/contactless IC card. This data communication apparatus has a memory area including a data accumulating memory (e.g., an EEPROM) and a data processing unit. This data communication apparatus further has a data communications function. In the case of, for example, a cell phone, an external storage medium, such as an IC card incorporating an IC chip, may be removably mounted to the cell phone. Additionally, the IC chip may include a subscriber identity module (SIM) function for storing the subscriber information provided by a cell phone carrier. The data communication apparatus can carry out data communication via an information communication network, such as the Internet, or can directly communicate data with an external apparatus either wired or wirelessly.

[0023]

The embodiments of present invention provide a service that ensures security of, for example, the exchange of value information using the tamper resistant and authenticating function of an IC card. More particularly, the present invention reduces the card issuing load of service providers by allowing the plurality of services to share a single memory space inside the IC card. Also, the present invention reduces the number of cards that a user carries and manages.

[0024]

Here, when a plurality of service providers share a single memory area and some service provider is allowed to access a memory space for a different provider, value information set by each service provider may be accessed by other unauthorized service providers.

[0025]

According to embodiments of the present invention, file systems for a plurality of service providers are allocated in a single memory space, and one data communication apparatus can be shared by the service providers so as to provide a plurality of services. By separating the memory area into a plurality of file systems, the border between the file systems functions as a firewall, thus appropriately preventing one of the file systems (i.e., one of the service providers) from being accessed (intruded) by the other file systems.

[0026]

Initially, the entire memory area in an IC card is managed by an original card issuer of the IC card. When a service provider other than the original IC card issuer separates the memory area to generate a new file system, the service provider is required for the authority of separating the memory area and the authentication by the original IC card issuer.

[0027]

For example, when the second service provider, which is

a new service provider, desires to separate the file system in a memory area of an IC card, the second service provider requests permission from the original card issuer, which is the first service provider, to use a memory area in advance. Subsequently, in order to give the permission to separate a free memory area into a file system, the original card issuer acquires a "separate element package" that is required for separating the file system from a separating engineering manager.

[0028]

Here, the separating engineering manager assigns an area key K_{ri} of the file system newly generated by the separation and a system code SC_i . The separating engineering manager then encrypts a data block including such data by using a separating authority key K_d to generate the separate element package and delivers this separate element package to the card issuer. Since the card issuer does not have the separating authority key K_d , the card issuer can neither decrypt nor falsify the delivered separate element package.

[0029]

The card issuer further encrypts the data block including the received separate element package and the size (the number of blocks) of the separate area that the new service provider is permitted to use using an issuer key K_I

that exclusively belongs to the card issuer so as to generate a separate package. Since the separate package is encrypted using the card issuer key K_I , a third party can neither decrypt the separate package nor falsify the size of the separate area.

[0030]

The card issuer requests the separation of the file system using this separate package. When the separating request is received by an operating system of the IC card, the separate package is delivered to the file system of the card issuer on the basis of the area ID contained in an argument. The separate package is then decrypted using the card issuer key K_I . Subsequently, the separate element package and the size of the separate area are retrieved.

[0031]

Upon receiving the separate element package and the size of the separate area from the file system of the card issuer, the operating system of the IC card decrypts the separate element package using the separating authority key K_d to retrieve the area key K_{I1} immediately after the separation (a default issuer key of the second service provider) and the system code SC_i . Thereafter, the operating system separates a memory area of the requested size from the unused area. Furthermore, the operating system sets the issuer key K_{I1} and the system code SC_i for

this area to define this area as a new file system.

[0032]

After the memory space is separated, in order to access the file system, the authentication by the service provider of the file system is required in place of the authentication by the original IC card issuer. Therefore, when using each service, a user of the IC card can obtain ease of use as if the IC card were directly issued by the service provider of the service that the user is currently using.

[0033]

By repeating such a separating operation, a plurality of file systems coexist in the memory area of the IC card. The separation of the file system is considered to be a virtual card issuing operation.

[0034]

Each of the file systems in the memory space has area identification information and an external access includes a package encrypted using the issuer key of the file system. In such a case, upon receiving an external access having the area identification information and the package in the form of arguments of the external access, the controlling means delivers the package to the corresponding file system on the basis of the area identification information, and the file system decrypts the package using the issuer key of the file

system.

[0035]

Accordingly, the service provider having the file system can communicate with the file system while keeping secret from a control system of the IC card and the original card issuer by using the issuer key of the service provider. That is, the service provider can analyze, manage, and deal with the threat to security independently from the original card issuer.

[0036]

Additionally, when separating a new file system, the controlling means sets the system code of the file system together with the issuer code and the area identification information.

[0037]

In this case, each service provider issues a request for acquiring the area identification information using the system code of the service provider as an argument of the request. In addition, in response to the request, the controlling means performs polling on each of the file systems to acquire the area identification information from the corresponding file system and returns the acquired area identification information to the requester. The service provider can manage only the system code thereof. When the service provider accesses the file system, the service

provider can sequentially acquire the area identification information and can issue the access request using the area identification information as an argument of the access request.

[0038]

Furthermore, after the service provider has acquired the file system thereof in the memory space, the controlling means may rewrite the default issuer key and the system code when the default issuer key and the system code are set at the separating time. Thus, the service provider can analyze, manage, and deal with the threat to security concerning the file system of the service provider independently from the separating engineering manager who manages the separation of the file system.

Advantages

[0039]

According to embodiments of the present invention, an excellent data communication apparatus and method for managing a memory of the data communication apparatus can be provided that can store electronic value information in the memory area and securely exchange the information for, for example, electronic payment.

[0040]

Additionally, according to embodiments of the present invention, an excellent data communication apparatus and method for

managing a memory of the data communication apparatus can be provided that can provide a user with the ease of use as if an IC card were directly issued by a service provider of the service that the user is currently using and that has a mechanism to securely manage information about a plurality of service providers in a memory area so that the plurality of service providers can share one IC card.

[0041]

Furthermore, according to embodiments of the present invention, file systems of a plurality of service providers are allocated in a single memory area and the service providers share a single data communication apparatus. Thus, the present invention can provide an excellent data communication apparatus and method for managing a memory of the data communication apparatus that can provide a plurality of services using the single data communication apparatus.

[0042]

Further features and advantages of embodiments of the present invention will become apparent from the following detailed description of exemplary embodiments with reference to the attached drawings.

Best Mode for Carrying Out the Invention

[0043]

Embodiments of the present invention are now herein described in detail with reference to the accompanying

drawings.

[0044]

The present invention provides a service that ensures security of, for example, the exchange of value information using the tamper resistant and authenticating function of an IC card. More particularly, the present invention reduces the card issuing load of service providers by allowing a plurality of services to share a single memory space inside the IC card. Also, the present invention reduces the number of cards that a user carries and manages.

[0045]

Here, when a plurality of service providers share a single memory area and some service provider is allowed to access a memory space for a different provider, value information set by each service provider may be accessed by other unauthorized service providers.

[0046]

According to the present invention, file systems for a plurality of service providers are allocated in a single memory space, and one data communication apparatus can be shared by the service providers so as to provide a plurality of services. By separating the memory area into a plurality of file systems, the border between the file systems functions as a firewall, thus appropriately preventing one of the file systems (i.e., one of the service providers)

from being accessed (intruded) by the other file systems.

[0047]

Initially, the entire memory area in an IC card is managed by an original card issuer of the IC card. When a service provider other than the original IC card issuer separates the memory area to generate a new file system, the service provider is required for the authority of separating the memory area and the authentication by the original IC card issuer.

[0048]

After the memory space is separated, in order to access the file system, the authentication by the service provider of the file system is required in place of the authentication by the original IC card issuer. Therefore, when using each service, a user of the IC card can obtain ease of use as if the IC card were directly issued by the service provider of the service that the user is currently using.

[0049]

The basic concepts of noncontact data communication between an IC card and a card reader/writer are described next with reference to Figs. 1 and 2.

[0050]

Wireless data communication between a card reader/writer and an IC card is realized on the basis of the

principles of electromagnetic induction. Fig. 1 schematically illustrates the basic concepts of wireless data communication between a card reader/writer and an IC card. A card reader includes an antenna L_{RW} composed of a loop coil. By applying an electric current I_{RW} to the antenna L_{RW} , a magnetic field is generated around the antenna L_{RW} . On the other hand, a loop coil L_c is electrically formed around the IC card. At terminals of the loop coil L_c of the IC card, an induction voltage is caused by the magnetic field generated by the loop antenna L_c of the card reader/writer. The induction voltage is input to the terminals of the IC card connected to the terminals of the loop coil L_c .

[0051]

The coupling ratio between the antenna L_{RW} of the card reader/writer and the loop coil L_c of the IC card varies depending on the positional relationship therebetween. However, from a system perspective, the antenna L_{RW} of the card reader/writer and the loop coil L_c of the IC card form one transformer. Accordingly, the read/write operation of the IC card can be modeled as shown in Fig. 2.

[0052]

The card reader/writer modulates the electric current I_{RW} applied to the antenna L_{RW} so that a voltage V_0 induced in the loop coil L_c of the IC chip is modulated. Using this

phenomenon, the card reader/writer can transmit data to the IC card.

[0053]

Additionally, the IC card has a function to change the load between the terminals of the loop coil L_c in accordance with data to be returned to the card reader/writer (load switching). When the load between the terminals of the loop coil L_c varies, the impedance between the terminals of the antenna of the card reader/writer varies. Thus, the variance in the electric current I_{RW} passing through the antenna L_{RW} or a voltage V_{RW} of the antenna L_{RW} is produced. By demodulating this variance, the card reader/writer can receive the data returned from the IC card.

[0054]

That is, by varying the load of the antenna in accordance with the response signal to the inquiry signal from the card reader/writer, the IC card can modulate the amplitude of a signal appearing in a reception circuit of the card reader/writer. Thus, the IC card can communicate with the card reader/writer.

[0055]

The IC card may be a card data communication apparatus or may be an information communication apparatus (e.g., a cell phone) incorporating an integrated circuit chip having an IC card function. For simplicity, as used herein, either

one of the apparatus incorporating an IC card and the apparatus in which the IC card is removably mounted is also referred to as an "IC card". In addition, the integrated circuit chip having an IC card function is mounted in a mobile device (e.g., a cell phone or a PDA) and an information processing apparatus (e.g., a personal computer (PC)) in order to communicate data with an external apparatus. In such a case, the IC card includes an external peripheral interface in addition to the interface for communicating with the card reader/writer wired or wirelessly.

[0056]

Fig. 3 illustrates the hardware configuration of a data communication apparatus according to the present invention. The data communication apparatus has an IC card function that allows the internal nonvolatile memory thereof to be accessed when a communication antenna is attached and a reader/writer function that supplies an external apparatus having an IC card function with electric power in order to achieve data exchange. The data communication apparatus incorporates an IC chip including a card function analog circuit 30, a data processing unit 40, and a card reader/writer function analog circuit 50. In an example shown in the drawing, the IC card has the card read/write function. However, this card read/write function is not an

essential feature of the present invention.

[0057]

In the card function analog circuit 30, carrier waves received by an antenna 32 are rectified by a rectifier 31 and are delivered to a signal processing unit 44 of the data processing unit 40 and a logic circuit 38 via a serial regulator 33.

[0058]

The logic circuit 38 starts in response to a start signal input from a start-signal input terminal P_{on} . The logic circuit 38 controls the voltage from the serial regulator 33 and the voltage input from a power supply terminal V_{DD} so as to supply a power supply voltage appropriate for the IC card.

[0059]

The serial regulator 33 remains the output voltage constant regardless of the level of the input voltage. That is, if the input voltage is high, the serial regulator 33 increases the internal impedance so as to maintain the voltage constant. In contrast, if the input voltage is low, the serial regulator 33 decreases the internal impedance so as to maintain the voltage constant.

[0060]

A voltage detector 39 monitors the input terminal voltage from a power-supply monitoring circuit connection

terminal V_{BT} connected to the logic circuit 38. If the voltage of an external power supply drops below a predetermined voltage, the voltage detector 39 outputs a signal for disabling the use of the external power supply to the logic circuit 38.

[0061]

Additionally, in the card function analog circuit 30, a carrier-wave detector 34 determines whether radio waves input from the antenna 32 include carrier waves. If the radio waves input from the antenna 32 include the carrier waves, a carrier wave detection signal VR is output to the logic circuit 38. The logic circuit 38 can further output a signal indicating that the carrier waves are detected to the data processing unit 40.

[0062]

A clock extractor 35 extracts a clock from the radio waves input from the antenna 32 and delivers this clock to a clock selector 36. A clock oscillator 37 is composed of, for example, a quartz resonator disposed outside the IC card. The clock oscillator 37 generates a clock of the driving frequency used for the IC card and delivers the clock to the clock selector 36. The clock selector 36 selects one of the clock delivered from the clock extractor 35 and the clock delivered from the clock oscillator 37 and delivers the selected clock to each component of the IC card.

[0063]

The card reader/writer function analog circuit 50 includes a transmission amplifier 51, a reception signal detector 53, a reception amplifier filter 54, and transmission and reception antennas 52 and 55.

[0064]

When transmitting data, the signal processing unit 44 of the data processing unit 40 modulates and D/A-converts the data to generate a transmission signal that is up-converted to an analog base-band. The transmission signal is output from the antenna 51 via the transmission amplifier. A signal received by the antenna 52 is detected by the reception signal detector 53 and is amplified by the reception amplifier 54. The signal is then delivered to the signal processing unit 44. The signal processing unit 44 down-converts the signal to the analog base-band signal. The signal processing unit 44 then D/A-converts and demodulates the signal to reproduce the digital data.

[0065]

The card read/write operation between the IC card and the card reader/writer is the same as that described in relation to Figs. 1 and 2.

[0066]

The data processing unit 40 includes, in addition to the above-described signal processing unit 44, a central

processing unit (CPU) 45, a data encryption engine 46 using, for example, the data encryption standard (DES), an error correction unit 47 using, for example, the cyclic redundancy check (CRC), a random access memory (RAM) 41, a read only memory (ROM) 42, an electrically erasable and programmable ROM (EEPROM) 43, a UART interface 48, and an I²C interface 49. All the above-described components are connected to each other via an internal bus.

[0067]

The CPU 45 serves as a main controller that performs overall control of the operation of the IC card. The CPU 45 executes program code stored in, for example, the ROM 42 (or the EEPROM 43) in the execution environment (described below) provided by an operating system (OS) of the IC card. For example, the CPU 45 executes an application about data to be transmitted and data received via the card function analog circuit 30 and the card reader/writer function analog circuit 50.

[0068]

The signal processing unit 44 modulates, D/A-converts, and up-converts data to be transmitted via the card function analog circuit 30 and the card reader/writer function analog circuit 50. The signal processing unit 44 also down-converts, A/D-converts, and demodulates the received data.

[0069]

The DES engine 46 encrypts and decrypts data to be transmitted and data received via the card function analog circuit 30 and the card reader/writer function analog circuit 50 using a secret key encryption scheme based on a publicly recognized algorithm.

[0070]

The CRC 47 performs a cyclic redundancy check on data received via the card function analog circuit 30 and the card reader/writer function analog circuit 50.

[0071]

The UART 48 and the I²C interface serve as an external wired interface for connecting the IC card to an external apparatus, such as a cell phone, a PDA, or a personal computer (not shown in Fig. 3). The UART (universal asynchronous receiver transmitter) 48 converts parallel signals to a serial signal or converts a serial signal to parallel signals in a computer.

[0072]

The RAM 41 is a writable memory unit. The CPU 41 executes a program using the RAM 41 as a work area. A memory space provided by the RAM 41 is addressable. The CPU 41 and each component on the internal bus can access the memory space.

[0073]

The EEPROM 43 is a nonvolatile memory unit for which an

erase operation can be performed and new data written. As used herein, the memory area in the IC card is basically referred to as a writable area in the EEPROM 43.

[0074]

The memory area includes at least one file system. In an initial state, the memory area is managed by a single file system managed by the original IC card issuer. Subsequently, a service provider other than the IC card issuer separates the memory area to generate a new file system. The file separation from the memory space in the EEPROM 43 and an access operation after the file separation are described in detail below.

[0075]

Fig. 4 is a schematic illustration of the structure of a control system of the memory area in the IC card according to the present invention. As shown in Fig. 4, this control system is basically implemented in the form of a subsystem of the operating system. The control system includes a protocol interface module, and an OS core module, and a file system.

[0076]

The protocol interface module handles an access request to the file system from an external apparatus via the external peripheral interface, such as the UART 48, and an access request to the file system from the card

reader/writer via the contactless IC card interface.

[0077]

The OS core module encodes and decodes data exchanged with the file system, corrects the error of the data using the CRC, manages the number of data updates for each block of the EEPROM 43, checks a PIN, and performs mutual authentication.

[0078]

Furthermore, the OS core module provides several application programming interfaces (APIs) for accessing the file system (e.g., APIs for PIN checking and mutual authentication during file access and APIs for file reading/writing).

[0079]

A physical access is performed to the EEPROM 43 serving as a file system entity. The physical memory access operation to a memory device including an EEPROM is well known to those skilled in the art. Therefore, a description thereof is not provided here.

[0080]

A memory area expanded on the EEPROM 43 includes at least one file system. In an initial state, the memory area is managed by a single file system managed by the original IC card issuer. When a service provider other than the original IC card issuer separates the memory area to create

a new file system, the service provider is required for the authority of separating the memory area and authentication by the original IC card issuer. After the memory space is separated, in order to access the file system, authentication of the file system by the service provider is required in place of authentication by the original IC card issuer. The separation of the file system is considered to be a virtual card issuing operation.

[0081]

The OS manages a separating authority key K_a for permitting the separation. Additionally, the OS manages an issuer key K_i of the issuer (the original IC card issuer or the service provider which has separated the file), a system code, and an area ID for identifying a file area for each file system.

[0082]

To access the file system, a procedure including a request for an area ID by polling and mutual authentication is required. The issuer of the file system (the card issuer for the original file or the service provider which uses the file system after being separated) poles the file systems using a system code that the issuer of the file system has in the form of an argument so as to acquire the area ID of a memory area corresponding to the file system. Subsequently, mutual authentication is performed using this area ID and an

issuer key K_I . If the mutual authentication is successfully performed, the access to the file system is permitted. The access to the file system is performed through encrypted communication using the issuer key K_I that is unique to the file system for the issuer. Accordingly, a different file system cannot read data from the file system without permission. In addition, an issuer other than the issuer of the file system cannot read data from and write data to the file system without permission.

[0083]

Fig. 5 is a schematic illustration of the structure of a service providing system for managing electronic money, an electronic ticket, and other value information using a relatively high-capacity IC card.

[0084]

As shown in Fig. 5, for example, a system 1 includes an issuer communications apparatus 11 used by an IC card issuer 21, a manager communications apparatus 12 used by a card storage area manager 22, a manufacturer communications apparatus 13 used by a manufacturer 23 of the apparatus, and a storage area separating apparatus 14 and a management file registration apparatus 15 used by a card storage area user 24.

[0085]

In the system 1, when the IC card issuer 21 issues an

IC card 16 to a card holder 26, file data related to a service provided by the card storage area user 24 is stored in the IC card 16 on the basis of a predetermined condition. Thus, the card holder 26 can receive the services from the IC card issuer 21 and the card storage area user 24 using the one IC card 16.

[0086]

As shown in Fig. 5, in the system 1, the issuer communications apparatus 11, the manager communications apparatus 12, the manufacturer communications apparatus 13, the storage area separating apparatus 14, and the management file registration apparatus 15 are connected to each other via a network 17.

[0087]

The IC card issuer 21 issues the IC card 16 to provide its own service using the IC card 16.

[0088]

Upon receiving a request from the IC card issuer 21, the card storage area manager 22 performs a service to lend a storage area that is not used by the IC card issuer 21 in a storage unit (semiconductor memory) of the IC card 16 issued by the IC card issuer 21 to the card storage area user 24.

[0089]

The manufacturer 23 manufactures the storage area

separating apparatus 14 in response to a request from the card storage area manager 22 and delivers the storage area separating apparatus 14 to the card storage area user 24.

[0090]

The card storage area user 24 requests the card storage area manager 22 to allow the card storage area user 24 to use a memory area of the IC card 16 and provides the service of the card storage area user 24. The card storage area user 24 corresponds to the above-described service provider which separates the memory area and creates a new file system. The card storage area user 24 provides its own service by using its own file system.

[0091]

The card holder 26 receives the IC card 16 from the IC card issuer 21 so as to use a service provided by the IC card issuer 21. When the card holder 26 desires to receive the service provided by the card storage area user 24 after the IC card 16 is issued, the card holder 26 stores file data related to the service provided by the card storage area user 24 in the IC card 16 using the storage area separating apparatus 14 and the management file registration apparatus 15. Thereafter, the card holder 26 can begin using the service provided by the card storage area user 24.

[0092]

To provide a service from the IC card issuer 21 and a

service from the card storage area user 24 using one IC card 16, the system 1 has a configuration so that unauthorized person cannot read data from and cannot write data to the storage area storing file data related to the service provided by the IC card issuer 21 and the card storage area user 24.

[0093]

As its name implies, the IC card 16 may be a card-type data communication apparatus. Alternatively, the IC card 16 may be realized as a cell phone (or a different mobile device or a CE device) incorporating a semiconductor chip having the IC card function.

[0094]

Although, the foregoing description is made with reference to one IC card issuer 21, one card storage area user 24, and one card holder 26 in Fig. 5, each one may be plural.

[0095]

In this embodiment, file systems for a plurality of service providers are allocated in a single memory area of the IC card. Also, a single data communication apparatus is shared by the service providers so as to provide a plurality of services. This separate file system configuration can provide the management of a memory area available to a specific service provider that has a permission of an

original card issuer and memory areas for a plurality of the service providers that have permission from the original card issuer as well as a memory area available to the original card issuer.

[0096]

In particular, when a plurality of file systems each being available to a service provider are managed in addition to the file system available to the original card issuer, the border between the file systems functions as a firewall, thus appropriately preventing one of the file systems (i.e., one of the service providers) from being accessed (intruded) by the other file systems.

[0097]

A method for managing the memory area of the IC card is now herein described with reference to Figs. 6 to 9.

[0098]

Fig. 6 illustrates the memory area in which an original card issuer manages only the original card issuer's file system. A system code SC1 is assigned to the original card issuer by a management mechanism of a system code. When an external apparatus or a program accesses the file system of the card issuer, the external apparatus or the program uses "SC1" as an identification code (i.e., an argument of a request command).

[0099]

Fig. 7 is a diagram illustrating that the card issuer can permit another memory area manager to rent or buy a certain amount of free space in the file system of the card issuer. In this stage, the file system in the memory space has not been separated yet. As long as the card issuer has free space in the card issuer's file system, the card issuer can permit a plurality of area managers to rent or buy a certain amount of free space. For example, in an implementation in which a file system is identified by a 4-bit system code, the file system can be separated into a maximum of sixteen separate areas (the file system can be separated up to fifteen times).

[0100]

Fig. 8 is a diagram in which another service provider separates a memory area permitted by the card issuer to generate a new file system. A system code SC2 is assigned to the new file system by the management mechanism of a system code. When an external apparatus or a program accesses the file system managed by the memory area manager (service provider), the external apparatus or the program uses "SC2" as an identification code (i.e., an argument of a request command).

[0101]

Fig. 9 is a diagram in which a common area manager separates a memory area permitted by the card issuer using a

system code SC0 of the common area. When an external apparatus or a program accesses the file system, which is a memory area managed by the common area manager, the external apparatus or the program uses the system code SC0 as an identification code (i.e., an argument of a request command).
[0102]

The procedure to generate a new file system by separating a memory area is described in detail next.
[0103]

Fig. 10 illustrates a pre-process of separating a file system. When a new service provider desires to separate the file system in a memory area of an IC card, the service provider requests permission from the card issuer to use a memory area. Subsequently, in order to give the permission to use the memory area (i.e., permission to separate the file system), the card issuer acquires a "separate element package" that is required for separating the file system from a separating engineering manager.
[0104]

The separating engineering manager corresponds to the card storage area manager 22 who manages the memory area in the IC card after manufacturing or delivering the IC card, whereas the new service provider corresponds to the card storage area user 14 (see Fig. 5).
[0105]

The separating engineering manager has authority to assign a system code to each file system in the memory area of the IC card and manages the separating authority key K_d stored in the operating system, which provides an execution environment of the IC card. The separating engineering manager assigns an area key K_{Ti} of the file system newly generated by the separation (an issuer key of the new service provider using this area (i.e., a virtual card issuer)) and a system code SC_i (where "i" denotes an index representing an i-th separate file system). The separating engineering manager then encrypts a data block including such data by using the separating authority key K_d to generate the separate element package and delivers this separate element package to the card issuer.

[0106]

Since the card issuer does not have the separating authority key K_d , the card issuer can neither decrypt nor falsify the delivered separate element package.

[0107]

The card issuer further encrypts the data block including the received separate element package and the size (the number of blocks) of the separate area that the new service provider is permitted to use using an issuer key K_I that exclusively belongs to the card issuer so as to generate a separate package.

[0108]

Since the separate package is encrypted using the card issuer key K_I managed by the card issuer and the file system of the card issuer, a third party can neither decrypt the separate package nor falsify the size of the separate area.

[0109]

After such a pre-process is performed, the card issuer acquires the separate package and requests the separation of the file system in the memory area of the IC card using this separate package. Here, the access to the file system is performed using the area ID of the file system as an argument. Since the card issuer knows only the system code, the card issuer performs polling on the IC card. Thus, the card issuer can acquire the area ID of the card issuer's file system.

[0110]

Fig. 11 illustrates the procedure performed by the card issuer to poll the IC card. However, the communication between the card issuer (or another external apparatus) and the IC card may be performed using a contactless short-range communication interface based on the electromagnetic induction described in relation to Figs. 1 and 2 or using a wired interface, such as the UART48 or I²C49 (hereinafter the same applies).

[0111]

The card issuer performs polling on the operating system, which is an execution environment of the IC card so as to request the area ID of a file system using a system code SC of the card issuer as an argument.

[0112]

When triggered by this request message, the mutual authentication procedure including a plurality of bi-directional communication operations is performed between the card issuer, which is a requester, and the operating system, which is an execution environment of the IC card. Thereafter, an area ID is returned to the card issuer as a return value. The configuration of the mutual authentication procedure is different depending on the specification of the IC card and is not directly related to a key feature of the present invention. As such, a detailed description thereof is not provided.

[0113]

The new service provider (i.e., the virtual card issuer) that acquired the new file system by the separation also performs the similar polling procedure to acquire an area ID that exclusively belongs to the new service provider.

[0114]

The card issuer issues a file-system separating request to the operating system of the IC card. This file-system separating request requires the area ID of the card issuer

and the separate package as the arguments. Since the separate package is encrypted using the card issuer key K_I , a third party cannot falsify the separate package. Fig. 12 illustrates the procedure of the separating request sent from the card issuer to the IC card. Fig. 13 illustrates a case in which the memory area of the IC card is separated and a new file system is generated. The communication between the card issuer and the IC card is performed using a contactless short-range communication interface based on electromagnetic induction or using a wired interface, such as the UART48 or I²C49.

[0115]

When the separating request is received by the operating system of the IC card, the separate package is delivered to the file system of the card issuer on the basis of the area ID in the argument. The separate package is then decrypted using the card issuer key K_I . Subsequently, the separate element package and the size (number of blocks) of the separate area are retrieved.

[0116]

Upon receiving the separate element package and the size of the separate area from the file system of the card issuer, the operating system of the IC card decrypts the separate element package using the separating authority key K_d to retrieve the area key K_{II} immediately after the

separation (the issuer key of the new service provider using this area (i.e., a virtual card issuer)) and the system code SC_i . Thereafter, the operating system separates a memory area of the requested size from the unused area of the card issuer. Furthermore, the operating system sets the issuer key K_{Ii} and the system code SC_i for this area to define this area as a new file system.

[0117]

After such a separating procedure of the file system is completed, the status is returned to the card issuer, which is the requester of the separation.

[0118]

Thus, the new service provider can acquire its own file system in the memory area of the IC card issued by a different card issuer. Therefore, the service provider can develop a service business as if the service provider issued its own IC card, that is, while being a virtual card issuer.

[0119]

However, in the initial state immediately after the separation, the issuer key K_{Ii} and the system code SC_i remain those set by the separating engineering manager. That is, for the new service provider, some of the security settings of its own file system depend on the separating engineering manager. Thus, the new service provider cannot independently analyze, manage, and deal with the threat to

security.

[0120]

Accordingly, after acquiring the file system in the memory area of the IC card, the new service provider is required to carry out a procedure for resetting the issuer key K_{Ii} and the system code SC_i . Additionally, the size of the separate area may be changed during the resetting of the issuer key K_{Ii} and the system code SC_i .

[0121]

Fig. 14 illustrates the procedure for resetting the issuer key K_{Ii} and the system code SC_i carried out after the new service provider has acquired the new service provider's file system in the memory area of the IC card. The communication between the new service provider and the IC card is performed using a contactless short-range communication interface based on electromagnetic induction or using a wired interface, such as the UART48 or I²C49.

[0122]

The service provider performs polling on the operating system serving as the execution environment of the IC card so as to issue an area ID request to the file system using the system code SC_i determined immediately after the separation as an argument.

[0123]

When triggered by this request message, the mutual

authentication procedure including a plurality of bi-directional communication operations is performed between the new service provider and the operating system, which is the execution environment of the IC card. Thereafter, the default area ID assigned by the separating engineering manager during the separation is returned to the service provider as a return value of the request. The configuration of the mutual authentication procedure is different depending on the specification of the IC card and is not directly related to a key feature of the present invention. As such, a detailed description thereof is not provided.

[0124]

After the mutual authentication procedure is completed, the service provider issues a change request to change the default issuer key K_{Ii} to the operating system of the IC card. This key change request is carried out using the default area ID and a key change package as arguments of the key change request. Since the key change package is encrypted using the default issuer key K_{Ii} , a third party cannot falsify the key change package.

[0125]

When the key change request is received by the operating system of the IC card, the key change package is delivered to the file system of the service provider on the

basis of the area ID in the argument. The key change package is then decrypted using the card issuer key K_{Ii} . Thus, the key change package is retrieved. Subsequently, the card issuer key K_{Ii} of the file system is changed to a card issuer key K_{Ii}' . The status of the change operation is returned to the service provider, which is the requester of the key change operation.

[0126]

Thereafter, the service provider issues a change request to change the default system code SC_i to the operating system of the IC card. This system-code change request is carried out using the default area ID and a system-code change package as arguments of the system-code change request. Since the system-code change package is encrypted using the new issuer key K_{Ii}' , a third party cannot falsify the system-code change package.

[0127]

When the system-code change request is received by the operating system of the IC card, the key change package is delivered to the file system of the service provider on the basis of the area ID in the argument. The system-code change package is then decrypted using the card issuer key K_{Ii}' . Thus, the system-code change package is retrieved. Subsequently, the default system code SC_i of the file system is changed to a system code SC_i' . The status of the change

operation is returned to the service provider, which is the requester of the system-code change operation.

[0128]

Thereafter, the service provider issues a change request to change the default area ID_i to the operating system of the IC card. This system-code change request is carried out using the default area ID and an area-ID change package as arguments of the system-code change request. Since the area-ID change package is encrypted using the new issuer key K_{II}' , a third party cannot falsify the system-code change package.

[0129]

When the area-ID change request is received by the operating system of the IC card, the area-ID change package is delivered to the file system of the service provider on the basis of the area ID in the argument. The area-ID change package is then decrypted using the card issuer key K_{II}' . Thus, the area-ID change package is retrieved. Subsequently, the default area ID_i of the file system is changed to an area ID_i' . The status of the change operation is returned to the service provider, which is the requester of the area-ID change operation.

[0130]

Thus, by setting the secure issuer key K_{II}' and the system code SC_i' for the file system, the new service

provider can analyze, manage, and deal with the threat to security independently from the original card issuer.

[0131]

As noted above, in this embodiment, the memory area of the IC card is separated into a plurality of file systems (see Fig. 15). The system code SC and the area ID are set for each file system. In addition, mutual authentication can be carried out using the issuer key K_{Ii} of a service provider (including the original card issuer) that uses the memory area. Thus, the service provider to which the file system is allocated can analyze, manage, and deal with the threat to security independently from the original card issuer.

[0132]

Additionally, when the service provider accesses the file system of the service provider, the procedure including the request for the area ID and the mutual authentication is basically required. The service provider performs polling on file systems using the system code that the service provider has in the form of an argument so as to obtain an area ID of the memory area for the corresponding file system. Subsequently, mutual authentication is performed using this area ID and the issuer key KI. If the mutual authentication is successfully completed, the service provider is allowed to access the file system.

[0133]

Furthermore, each service provider (including the original card issuer) packages a request command (e.g., a read request, a write request, a data-delete request, or a area/service registration request, which is described below) using the issuer key KI that exclusively belongs to the file system of the service provider and carries out an encryption communication using this package (see Fig. 16). Accordingly, a different file system cannot retrieve unrelated data and a third party cannot read data from and write data to the file system without permission.

[0134]

By repeating the separating operation of the memory area of the IC card, a plurality of file systems coexist, as shown in Fig. 15. The original card issuer and a service provider that acquired the service provider's file system on the IC card under the permission of the card issuer can arrange areas and services using the file system, as described below, in order to develop the business plan.

[0135]

The management in one file system is described below. Basically, the same operation is applied to each file system. It is assumed that, to operate the file system, the above-described area-ID request and mutual authentication have been performed in advance.

[0136]

In a file system, one or more applications, such as an external electronic value exchange including electronic payment, are allocated. A memory area allocated to an application is referred to as a "service memory area". Also, the use of the application, namely, the operation to access the service memory area corresponding to the application is referred to as a "service". Examples of the service include access for reading the memory, access for writing the memory, and the addition and subtraction of value information (e.g., electronic money).

[0137]

In order to restrict the user of an application, namely, the activation of the service depending on whether the user has the access authority, a security code (i.e., a PIN) is assigned to the application. The PIN is verified at a service start-up time. Additionally, the access to the service memory area is secured with appropriate encrypted communication in accordance with the security level of the application.

[0138]

In this embodiment, a hierarchy structure that is similar to a "directory" is introduced to each file system set in a memory area of the IC card. Each application allocated in the memory area can be registered to an "area"

in the desired layer.

[0139]

For example, a plurality of applications involved in a series of transactions or deeply related applications are registered to a service memory area in the same area (and the deeply related applications are further registered to the same parent area). Thus, the applications in the memory area and the area are organized. For the user, the applications are efficiently classified and organized.

[0140]

Additionally, a PIN can be set for each application in order to control the access authority for the file system in a hierarchical fashion. Furthermore, a PIN can be set for each area. For example, by inputting a PIN for some area, a user may obtain the access authority for all the applications in the area after the verification process and a mutual authentication process are successfully carried out. Accordingly, since, by inputting a PIN for some area only once, the user can obtain the access authority for all the applications involved in a series of transactions, an efficient access control can be provided. In addition, the ease of operation of the apparatus can be improved.

[0141]

Furthermore, a plurality of access authorities can be set for a service memory area, and a security code can be

set for each authority, namely, for each service executed in the service memory area. For example, different PINs are set for services activated in the same service memory area (e.g., "read" service and "read and write" service). In another example, different PINs are set for "increase" service and "decrease" service of electronic money or other value information. Furthermore, for some memory area, the following setting is possible: the input of a PIN is not required for a read operation; however, the input of a PIN is required for a write operation.

[0142]

Fig. 17 is a schematic illustration of the data structure of the file system. In an example shown in Fig. 17, a hierarchy structure that is similar to a "directory" is introduced to a memory space of the file system. That is, each application allocated to the memory area can be registered to a desired hierarchy area as a service memory area. For example, deeply related applications (e.g., applications used for a series of transactions) can be registered to the same area (and the deeply related areas can be further registered to the same parent area).

[0143]

In addition, each of the application (i.e., the service memory area) and the area allocated to the file system has a security code definition block. Therefore, a PIN can be set

for each application or each area. Furthermore, the access authority for the file system can be set on an application basis and on an area basis.

[0144]

Still furthermore, instead of setting one authority for a service memory area, a PIN can be set for each executed service. For example, different PINs are set for services "read" and "read and write" that are activated for the same service memory area. Also, different PINs are set for services "increase" and "decrease" of electronic money or other value information.

[0145]

A verification unit compares a PIN sent via the protocol interface (such as the contactless short-range communication based on electromagnetic induction or the UART48, or I²C49) with a security code set for an area allocated to each application or a directory or with a security code set for a service memory area, so that the access to the memory area having the equal security code is allowed. The memory area to which access is allowed is accessible via the protocol interface.

[0146]

As described above, in a file system, a variety of service memory areas that are allocated to applications are allocated, and one or more services that are applicable to

each service memory area are set. In this embodiment, access restriction is set on an area basis and on an application basis. In addition, a PIN is set for the type of services applied to an application so that access restriction can be set on a service basis.

[0147]

Fig. 18 illustrates the basic structure of the file system. As described in relation to Fig. 17, the hierarchy structure that is similar to a "directory" is introduced to each file system. A service memory area allocated to an application can be registered to an area in the desired layer. In the example shown in Fig. 18, one service memory area is registered in an area 0000 defined by an area definition block 0000.

[0148]

The service memory area in Fig. 18 is composed of at least one user block. The term "user block" refers to a minimum unit of data to which an access operation is ensured. A service defined by a service 0180 definition block, namely, a service 0108 can be applied to the service memory area.

[0149]

In addition to access restriction on an area basis and on an application basis, an access restriction can be set on a service basis by setting a security code for each type of service. Security code setting information for the service

to which the access restriction is applied is defined as a service dedicated to the security code (i.e., a security code service). In the example shown in Fig. 18, a security code for the service 0108 is defined as a security code service 0128 definition block. The details of the security code service are stored in a security code service data block.

[0150]

When the security code service for the service 0108 is enabled, the security code is required to be verified using the security code service 0128 before the service 0108 is activated and the read or write operation is performed on the user block of the service 0108. More specifically, when a read/write command with encryption is used, the security code for the service 0108, namely, the PIN for the service 0108 is verified before the mutual authentication is performed.

[0151]

In addition, a service memory area allocated to an application can be registered in an area in the desired layer, and the area can be layered (the deeply related areas are registered in the same parent area). In such a case, by setting a PIN for each area, the area can serve as a unit of the access restriction. Fig. 19 illustrates areas layered in memory space of the IC card 50. In the example shown in

Fig. 19, a different area 1000 defined by an area 1000 definition block is registered in an area 0000 defined by an area 0000 definition block.

[0152]

In the example shown in Fig. 19, two service memory areas are further registered in the area 1000. To one of the two service memory areas, a service 1108 defined by a service 1108 definition block and a service 110B defined by a service 110B definition block can be applied. As used herein, to define a plurality of different services for one service memory area is referred to as an "overlap service". In the overlap service, different services are applied to the same service area depending on the input PIN. Additionally, to the other one of the two service memory areas, a service 110C defined by a service 110C definition block can be applied.

[0153]

After a service set in a service memory area is activated, a read or write operation can be carried out on the user block of the service memory area. As described in relation to Fig. 18, a security code service can be defined for each service. In this case, if the security code service for the service is activated, the activation of the service is allowed after PIN verification using the security code service is completed.

[0154]

When a common PIN is required to be set for a plurality of services, an area including these services can be generated and a common security code service can be applied to this area.

[0155]

In the example shown in Fig. 19, a security code for the area 1000 is defined as a security code service 1020 definition block. The details of the security code service are stored in a security code service data block.

[0156]

When the security code service for the area 1000 is enabled (as will be described further below), the security code is verified using the security code service 1020. Thereafter, each service in the area 1000 is activated. Thus, a read or write operation can be performed on the user block of the service.

[0157]

Here, when a security code service is applied to the service in the area 1000 and the security code service is enabled, the read or write operation cannot be performed on the user block of the service until the security code verification using the security code service is completed.

[0158]

As shown in Figs. 18 and 19, a unique security code

service corresponding to the area and service for the security code verification is provided.

[0159]

Fig. 20 illustrates the procedure for registering an area and a service in a file system in the form of a flow chart.

[0160]

First, an area is defined in memory space (step S1).

[0161]

Subsequently, using a registration service command of a service, a service memory area for an application is allocated in the area. At the same time, a service applied to the service memory area is defined (step S2). In the registration service command, the number of user blocks in the service memory area is specified. To allocate a plurality of applications in the area, this step is repeatedly executed.

[0162]

To apply a security code to the service defined in the area, a security code service is registered using the registration service command of the service (step S3).

[0163]

The security code service is registered using the registration service command as for a normal service. However, to register the security code service, the area and

service subjected to the security code verification must be already registered. That is, if the area and service subjected to the PIN verification are not found, an error occurs during executing the registration service of the security code service. Additionally, since the security code service has only one security code service data block, which corresponds to a user block of a normal service, an error occurs if the number of user blocks other than one is specified in the registration service command at a service registration time.

[0164]

Furthermore, to set a security code that is common to all the services defined in the area, a common security code service is registered for this area using the registration service command of a service (step S4).

[0165]

It should be noted that the process at step S4 may be executed before the process at step S3 is executed.

[0166]

Still furthermore, to define a plurality of different services for one service memory area, an overlap service (see Fig. 19) is registered using the registration service command of a service (step S5).

[0167]

In addition, to apply a security code to the overlap

service, a security code service is registered using the registration service command of a service (step S6).

[0168]

In the example shown in Fig. 18, after a service memory area is allocated in the root area 0000 and the service 0108 applied to the service memory area is registered, a security code service applied to the service 0108 is registered.

[0169]

Additionally, in the example shown in Fig. 19, two service memory areas are allocated in the area 1000 under the root area 0000. Also, the services 1108 and 110C respectively applied to the two service memory areas are registered. Furthermore, the different service 110B is registered in one of the service memories as an overlap service. Although not shown, if a security code is required to be applied to the service memory area, a security code service is separately registered. In addition, if a common security code is required to be applied to the registered services 1108, 110B, and 110C, a common security code service is registered in the area 1000.

[0170]

When the service provider (including the original card issuer) wants to register an area and a service in a file system that is allocated to the service provider, the service provider issues an area registration request and a

service registration request to the operating system, which provides the execution environment of the IC card. Since these registration requests are sent with the encrypted communication after packaged using the issuer key K_i that exclusively belongs to the file system of the provider (see Fig. 16), a third party cannot read data from and write data to the file system without permission.

[0171]

Fig. 21 illustrates the procedure performed at step S1 shown in Fig. 20 by the service provider (including the original card issuer) to register an area in the service provider's file system. The communication between the service provider and the IC card is performed using a contactless short-range communication interface based on electromagnetic induction or using a wired interface, such as the UART48 or I²C49.

[0172]

The service provider performs polling on the operating system serving as an execution environment of the IC card and issues an area ID request to the file system using the system code SC of the file system as an argument.

[0173]

When triggered by this request message, the mutual authentication procedure including a plurality of bi-directional communication operations is performed between

the service provider and the operating system, which is the execution environment of the IC card. Thereafter, an area ID is returned to the service provider as a return value. The configuration of the mutual authentication procedure is different depending on the specification of the IC card and is not directly related to a key feature of the present invention. As such, a detailed description thereof is not provided.

[0174]

After the mutual authentication procedure is completed, the service provider issues an area registration request to register an area in the file system to the operating system of the IC card. This area registration request is carried out using the area ID and an area registration request package as arguments of the area registration request. Since the area registration request package is encrypted using the issuer key K_I of the service provider, a third party cannot falsify the area registration request package.

[0175]

When the area registration request is received by the operating system of the IC card, the area registration request package is delivered to the file system of the service provider on the basis of the area ID in the argument. The area registration request package is then decrypted using the card issuer key K_I of the service provider. Thus,

the area registration request package is retrieved. Subsequently, the area requested in the package is registered in the file system. The status of the registration operation is returned to the service provider, which is the requester of the registration operation.

[0176]

Fig. 22 illustrates the procedure performed at step S2 shown in Fig. 20 by the service provider (including the original card issuer) to register a service in the service provider's file system (or a particular area registered in the file system). The communication between the service provider and the IC card is performed using a contactless short-range communication interface based on electromagnetic induction or using a wired interface, such as the UART48 or I²C49.

[0177]

The service provider performs polling on the operating system serving as the execution environment of the IC card and issues an area ID request to the file system using the system code SC of the file system as an argument.

[0178]

When triggered by this request message, the mutual authentication procedure including a plurality of bi-directional communication operations is performed between the service provider and the operating system, which is the

execution environment of the IC card. Thereafter, an area ID is returned to the service provider as a return value. The configuration of the mutual authentication procedure is different depending on the specification of the IC card and is not directly related to a key feature of the present invention. As such, a detailed description thereof is not provided.

[0179]

After the mutual authentication procedure is completed, the service provider issues a service registration request to register a service in the file system (or a particular area registered in the file system) to the operating system of the IC card. This service registration request is carried out using the area ID and a service registration request package as arguments of the service registration request. Since the service registration request package is encrypted using the issuer key K_I of the service provider, a third party cannot falsify the service registration request package.

[0180]

When the service registration request is received by the operating system of the IC card, the service registration request package is delivered to the file system of the service provider on the basis of the area ID in the argument. The service registration request package is then

decrypted using the card issuer key K_I of the service provider. Thus, the service registration request package is retrieved. Subsequently, the service requested in the package is registered in the file system (or the particular area registered in the file system). The status of the registration operation is returned to the service provider, which is the requester of the registration operation.

[0181]

As shown in Figs. 18 and 19, by applying a PIN to the area or the service registered in the file system, an access control can be carried out on an area basis or on a service basis. Additionally, when a plurality of services (an overlap service) is registered in one service memory area, a plurality of access methods can be defined for the same service memory area by applying a PIN to each service.

[0182]

However, in this embodiment, when accessing the file access, the mutual authentication (as described above) using the issuer key is essential and the PIN verification process is optional. That is, only when the security code service for a service or an area is enabled, the security code verification is required before starting the service or accessing the area. In contrast, when the security code service is disabled, the security code verification is not required.

[0183]

The details of the PIN are written in the security code service data block of the security code service definition block. Fig. 23 is a schematic illustration of the data structure of the security code service data block. As shown in Fig. 23, the security code service data block includes a security code area, a storage area for the number of failed authentication attempts, a setting area of maximum allowed failed authentication attempts, a security code use selection area, and an access permission flag.

[0184]

Only when the PIN entered by the user is successfully verified, the access permission flag in the security code service data block for the corresponding service or area is set so that access to the service or area is allowed.

[0185]

The access permission flag is a flag indicating whether access to the corresponding application or directory is allowed or not. The service or area whose access permission flag is set is accessible. By default, the access permission flag of the service or area for which a PIN is required is set to "inaccessible". After the PIN verification operation and the mutual authentication operation using the issuer key of the file system are successfully carried out, the access permission flag is set

so that access is allowed. In addition, if the access permission flag is continuously set and the IC card is lost or stolen, the user could suffer monetary loss due to unauthorized use of the service or area. Therefore, the IC card may have a feature to automatically change from the accessible state to the inaccessible state in response to, for example, the absence of electromagnetic waves.

[0186]

In addition, when an invalid PIN is input, the number of failed authentication attempts is updated. If the number of failed authentication attempts exceeds the maximum allowed failed authentication attempts set in the setting area of maximum allowed failed authentication attempts, the start of the corresponding service or access to the corresponding area is inhibited.

[0187]

In general, once the input of the PIN is successful, the number of failed authentication attempts should be cleared. Thus, a malicious user is prevented from combing the security code. If the number of inputs of the PIN from the user accidentally exceeds the maximum allowed failed authentication attempts and the verification fails, only a manager of the IC card (e.g., the separating engineering manager or the original card issuer) may clear the number of failed authentication attempts. To authenticate the manager,

authentication using a private key, which is described below, may be employed, for example.

[0188]

Fig. 24 illustrates the procedure for controlling the start of a service or access to an area in accordance with the security code input from the user in the form of a flow chart.

[0189]

When a user inputs a security code (step S11), the security code service data block of the security code service definition block is accessed to verify the security code (step S12).

[0190]

If the PIN in the security code service data block is equal to the PIN input by the user, the access permission flag in the security code service data block is set so that the corresponding service or area becomes accessible (step S13).

[0191]

For example, by placing an IC chip above a reader/writer, a PIN input via a user interface of an external apparatus (not shown) connected to the reader/writer can be transmitted to the IC card using a contactless short-range communication interface based on electromagnetic induction.

[0192]

As shown in Fig. 24, when the access authority to the application and the directory is controlled using the PIN, a malicious user could break the security wall by combing the PIN (in particular, in the case where a short-digit number is used for the security code). Accordingly, in this embodiment, the maximum allowed failed authentication attempts is set in the security code definition area so that an application or directory whose number of failed authentication attempts exceeds the maximum allowed failed authentication attempts becomes inaccessible. Thus, the access control is provided.

[0193]

Fig. 25 illustrates the procedure for controlling the access authority to a service and an area using the number of failed authentication attempts in the form of a flow chart.

[0194]

When a user inputs a PIN (step S21), each security code service definition block is accessed to verify the PIN (step S22).

[0195]

If the PIN input by the user is equal to the PIN in the security code service definition block, the access permission flag in the security code service data block is

set so that the corresponding service or area becomes accessible (step S23).

[0196]

However, if the PIN input by the user is not equal to the PIN in all of the security code service definition blocks, the number of failed authentication attempts in the security code definition area is updated (step S24).

Additionally, if the PIN input by the user is equal to the PIN in all of the security code service definition blocks and the authentication is successful, the number of failed authentication attempts is cleared to zero.

[0197]

At step S25, it is determined whether the updated number of failed authentication attempts exceeds the maximum allowed failed authentication attempts set in the security code definition area (step S25).

[0198]

If the number of failed authentication attempts exceeds the maximum allowed failed authentication attempts, the access permission flag in the security code definition area is cleared. Thus, the corresponding service or area becomes inaccessible (step S26). As a result, a malicious user is prevented from combing the PIN.

[0199]

In contrast, if the number of inputs of the PIN from

the user accidentally exceeds the maximum allowed failed authentication attempts and the verification of the security code fails, only a manager of the IC card (e.g., the separating engineering manager or the original card issuer) may clear the number of failed authentication attempts. To authenticate the manager, authentication using a private key may be employed, for example.

Industrial Applicability

[0200]

Although the invention has been shown and described with reference to the specific embodiments, it would be apparent to those skilled in the art that alternative embodiments may be made without departing from the spirit and scope of the invention as defined in the appended claims.

[0201]

While an embodiment of the present invention has been described with reference to an information management method of a memory area incorporated in an IC card, the present invention is not limited thereto. The present invention is applicable to a method of managing a memory incorporated in an apparatus other than an IC card in the same manner.

[0202]

That is, the forgoing description of the preferred embodiments of the invention has been presented only for the purpose of illustration and description and is not intended

to be exhaustive or to limit the invention to the precise forms disclosed. Therefore, the scope of the invention should be determined by the appended claims.

Brief Description of the Drawings

[0203]

Fig. 1 is a schematic illustration of the basic concepts of wireless data communication between a card reader/writer and an IC card based on electromagnetic induction;

Fig. 2 is a diagram in which a system including the card reader/writer and the IC card is modeled as a transformer;

Fig. 3 illustrates the hardware configuration of a data communication apparatus according to an embodiment of the present invention;

Fig. 4 is a schematic illustration of the structure of a control system of a memory area in the IC card according to an embodiment of the present invention;

Fig. 5 is a schematic illustration of the structure of a service providing system using the IC card;

Fig. 6 illustrates a memory area in which an original card issuer manages only the file system of the original card issuer;

Fig. 7 is a diagram illustrating that the card issuer can permit an area manager to rent or buy a certain amount

of free space of the file system of the card issuer;

Fig. 8 is a diagram in which another service provider separates a memory area permitted by the card issuer to generate a new file system;

Fig. 9 is a diagram in which a common area manager separates a memory area permitted by the card issuer using a system code SC0 of the common area;

Fig. 10 illustrates a pre-process of separating a file system;

Fig. 11 is a sequence diagram illustrating the procedure performed by the card issuer to poll the IC card;

Fig. 12 is a sequence diagram illustrating the procedure of the separating request sent from the card issuer to the IC card;

Fig. 13 illustrates a case in which the memory area of the IC card is separated and a new file system is generated;

Fig. 14 is a sequence diagram illustrating the procedure for resetting an issuer key KI_i and a system code SC_i carried out by a new service provider after the new service provider has acquired the file system thereof on the memory area of the IC card;

Fig. 15 is a schematic illustration of the structure of a memory area of the IC card in which a plurality of file systems coexist by repeating a separating operation;

Fig. 16 is a schematic illustration of the structure of

a request command packaged using an issuer key;

Fig. 17 is a schematic illustration of a directory structure in the file system;

Fig. 18 illustrates the basic structure of the file system;

Fig. 19 illustrates areas layered in a memory space of an IC card 50;

Fig. 20 is a flow chart illustrating the procedure for registering an area and a service in a file system;

Fig. 21 illustrates the procedure performed by a service provider (including an original card issuer) to register an area in the file system of the service provider;

Fig. 22 illustrates the procedure performed by a service provider (including the original card issuer) to register a service in the file system of the service provider;

Fig. 23 is a schematic illustration of the data structure of a security code service data block;

Fig. 24 is a flow chart illustrating the procedure for controlling the activation of a service or the access authority to an area in accordance with a security code input from a user; and

Fig. 25 is a flow chart illustrating the procedure for controlling the access authority to a service and an area on the basis of the number of failed PIN input attempts.

Reference Numerals

[0204]

- 11 issuer communications apparatus
- 12 manager communications apparatus
- 13 manufacturer communications apparatus
- 14 storage area separating apparatus
- 15 management file registration apparatus
- 16 IC card
- 17 network
- 21 card issuer
- 22 card storage area manager
- 23 manufacturer of apparatus
- 24 card storage area user
- 26 card holder
- 30 card function analog circuit
- 31 rectifier
- 32 antenna
- 33 serial regulator
- 34 carrier-wave detector
- 35 clock extractor
- 36 clock selector
- 37 clock oscillator
- 38 logic circuit
- 39 voltage detector
- 40 data processing unit

- 41 RAM
- 42 ROM
- 43 EEPROM
- 44 signal processing unit
- 45 CPU
- 46 data encryption engine
- 47 error correction unit
- 48 UART interface
- 49 I²C interface
- 50 reader/writer function analog circuit
- 51 transmission amplifier
- 52 transmission antenna
- 53 reception signal detector
- 54 reception amplifier filter
- 55 reception antenna
- 100 data communication apparatus

CLAIMS

1. A data communication apparatus having a memory space, the data communication apparatus managing the memory space by separating the memory space into one or more file systems, the apparatus comprising:

controlling means for holding a separating authority key and managing the access to the file system in the memory space; and

a first file system allocated to a first service provider in the memory space, the first file system holding an issuer key of the first service provider;

wherein, upon receiving, from a second service provider requesting an allocation of a new file system, a separate package generated by encrypting, using the issuer key of the first service provider, a data block containing a separate element package generated by encrypting an issuer key of the second service provider using the separating authority key and information on the new file system, the first file system decrypts the received separate package using the issuer key of the first service provider and retrieves the separate element package and the information on the new file system, and wherein the controlling means decrypts the separate element package using the separating authority key, retrieves the issuer key of the second service provider,

separates a free area of the memory space in accordance with the information on the new file system, and allocates the separated memory area to a second file system holding the issuer key of the second service provider.

2. The data communication apparatus according to Claim 1, wherein each of the file systems in the memory space has area identification information, and wherein, upon receiving an external access having the area identification information on a file system to be accessed and a package encrypted using the issuer key of the file system in the form of arguments of the external access, the controlling means delivers the package to the corresponding file system on the basis of the area identification information, and wherein the file system decrypts the package using the issuer key of the file system.

3. The data communication apparatus according to Claim 2, wherein each of the allocated file systems in the memory space has a system code, and wherein, when separating a new file system in response to the reception of the separate package, the controlling means sets the system code of the file system together with the issuer code and the area identification information.

4. The data communication apparatus according to Claim 3, wherein, when the service provider issues a request for acquiring area identification information using the system code of the service provider as an argument of the request after acquiring the file system, the controlling means performs polling on each of the file systems on the basis of the system code in the request to acquire the area identification information from the corresponding file system and returns the acquired area identification information to the requester.

5. The data communication apparatus according to Claim 3, wherein, in response to a request from the second service provider after the second service provider has acquired the file system, the controlling means rewrites the issuer key and the system code set in the second file system at the separating time.

6. The data communication apparatus according to Claim 1, wherein each of the file systems in the memory space has area identification information, and wherein, upon receiving, from the service provider after the service provider has acquired the file system, an external access having the area identification information and a package of an access request to the file system encrypted using the issuer key of

the service provider in the form of arguments of the external access, the controlling means delivers the encrypted package to the corresponding file system on the basis of the area identification information.

7. A method for managing a memory of a data communication apparatus, the data communication apparatus having a memory space and managing the memory space by separating the memory space into one or more file systems, wherein a separating authority key for authenticating authority to separate the file system and a first file system for authenticating access authority using an issuer key of a first service provider are provided in the memory space, the method comprising the steps of:

receiving, from a second service provider requesting an allocation of a new file system, a separate package generated by encrypting, using the issuer key of the first service provider, a data block containing a separate element package generated by encrypting an issuer key of the second service provider using the separating authority key and information on the new file system;

decrypting the received separate package using the issuer key of the first service provider and retrieving the separate element package and the information on the new file system; and

decrypting the separate element package using the separating authority key, retrieving the issuer key of the second service provider, separating a free area of the memory space in accordance with the information on the new file system, and allocating the separated memory area to a second file system holding the issuer key of the second service provider.

8. The method for managing a memory of a data communication apparatus according to Claim 7, wherein each of the file systems in the memory space has area identification information, and wherein an external access includes the area identification information on a file system to be accessed and a package encrypted using the issuer key of the file system in the form of arguments, and wherein the method further comprises the steps of receiving an external access request to the file system having area identification information and a package as arguments of the external access request, delivering the package to the corresponding file system on the basis of the area identification information, and decrypting the package using the issuer key of the file system by the file system.

9. The method for managing a memory of a data communication apparatus according to Claim 8, wherein each

of the allocated file systems in the memory space has a system code, and wherein the method further comprises the steps of setting the system code of the file system together with the issuer code and the area identification information when separating a new file system in response to the reception of the separate package.

10. The method for managing a memory of a data communication apparatus according to Claim 9, further comprising:

issuing, from the service provider, a request for acquiring area identification information using the system code of the service provider as an argument of the request after acquiring the file system; and

performing polling on each of the file systems on the basis of the system code in the request to acquire the area identification information from the corresponding file system and returning the acquired area identification information to the requester.

11. The method for managing a memory of a data communication apparatus according to Claim 9, further comprising the steps of issuing, from the second service provider, a request for rewriting the issuer key and the system code set in the second file system at the separating

time after the second service provider has acquired the file system of the second service provider in the memory space and rewriting the issuer key and the system code set in the second file system at the separating time in response to the rewriting request.

12. The method for managing a memory of a data communication apparatus according to Claim 7, wherein each of the file systems in the memory space has area identification information, and wherein the method further comprises the steps of receiving, from the service provider, an access request including the area identification information and a package of an access request to the file system of the service provider encrypted using the issuer key of the service provider in the form of arguments of the access request after the service provider has acquired the file system, and delivering the package to the corresponding file system on the basis of the area identification information contained in the arguments of the access request from the service provider.