

STORAGE MEDIUM, READ/WRITE APPARATUS, CARD SYSTEM, ENCRYPTION
KEY UTILIZATION METHOD, STATION SERVICE SYSTEM, AND CARD
ISSUING APPARATUS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a storage medium for storing data; a read/write apparatus for reading data from or writing data to the storage medium; a card system using the storage medium and the read/write apparatus; an encryption key utilization method suitable for use with the card system; a station service system, such as an automatic ticket examination machine, which uses the elements; and a card issuing machine.

2. Description of the Related Art

In a case where a card, corresponding to a storage medium, is subjected to processing for payment or receipt-of-money through use of a read/write apparatus of an automatic fare collection machine, the security of the card must be ensured. For this reason, mutual authentication between the card and the read/write apparatus is usually effected, and communication between the card and the read/write apparatus is encrypted. Here, the expression "mutual authentication" means that the card determines whether or not the read/write apparatus with which the card is to communicate is genuine and that the read/write apparatus determines whether or not the card to which the read/write apparatus is to communicate is valid. The card usually determines the read/write apparatus to be genuine by means of checking whether or not the read/write apparatus uses an appropriate encryption key, and vice versa.

In the field of encryption processing, there is a system

9904420-8

in which an identical encryption key (i.e., a common encryption key) is used for all the cards and the read/write apparatus. This type of system suffers a drawback in that if the common encryption key is leaked, the security of the entire system is compromised.

To eliminate the drawback, another system enhances security by storing a plurality of encryption keys in the card and the read/write apparatus. When the read/write apparatus authenticates the card by means of encryption, any one of the plurality of encryption keys is used randomly.

This system also disadvantageously involves a risk of all the encryption keys being intercepted during the course of random use of the encryption keys. Particularly, in a case where contactless communication is established between the card and the read/write apparatus, the risk of compromise is increased. A conceivable measure to eliminate the risk is to change all the plurality of encryption keys to other encryption keys in unison. However, changing of the encryption keys in unison is virtually impossible in view of the fact that a great number of cards are issued and used.

SUMMARY OF THE INVENTION

The present invention has been conceived in consideration of the above-described technical problem, and an object of the present invention is to enable updating of an encryption key, as needed; for example, periodic updating of an encryption key or updating of an encryption key in danger of being cracked, without involving random use of all encryption keys, as well as to eliminate a necessity for changing in unison a plurality of encryption keys stored in a storage medium.

To achieve the foregoing object, the present invention has the following configuration.

According to a first aspect of the present invention, there is provided a storage medium configured so as to effect authentication and establish communication with a read/write apparatus through use of an encryption key, the storage medium comprising:

encryption key storage means for storing a plurality of encryption keys;

encryption key selection means for selecting any one from among the plurality of encryption keys stored in the encryption key storage means; and

encryption key update means for updating the thus-selected encryption key by means of a command transmitted from the read/write apparatus.

Here, the expression "update" represents that the encryption key that is currently used is changed to another of the plurality of encryption keys and the thus-selected encryption key is used. Every time the encryption key is updated, another of the plurality of encryption keys is used in lieu of the encryption key that has been used before this time.

Communication established between the storage medium and the read/write apparatus may be wired or wireless.

Preferably, the read/write apparatus rewrites at least one of the plurality of encryption keys stored in the encryption key storage means.

According to a second aspect of the present invention, there is provided a read/write apparatus configured so as to effect authentication and establish communication with a

storage medium through use of an encryption key; the apparatus comprising:

encryption key storage means for storing a plurality of encryption keys;

encryption key selection means for selecting any one from among the plurality of encryption keys stored in the encryption key storage means;

encryption key awareness means for becoming aware of, on the basis of a response from the storage medium, whether or not the encryption key that is currently used by the storage medium corresponds to an encryption key used in the past by the read/write apparatus; and

encryption key update command transmission means which transmits a command for updating the encryption key of the storage medium when the encryption key currently used by the storage medium corresponds to an encryption key used in the past.

Preferably, the read/write apparatus comprises encryption key changing means for changing the encryption key to be used by the read/write apparatus, in response to a command issued by a higher-level apparatus.

Preferably, the storage medium rewrites at least one of the plurality of encryption keys stored.

According to a third aspect of the present invention, there is provided a card system comprising:

a card corresponding to the storage medium as defined in the first aspect; and

the read/write apparatus as defined in any one of the first and second aspects;

wherein if the encryption key currently used by the card

corresponds to an encryption key used by the read/write apparatus in the past, the encryption key of the card is updated, and then mutual authentication between the card and the read/write apparatus is effected through use of the thus-updated encryption key.

According to a fourth aspect of the present invention, there is provided an encryption key utilization method comprising the steps of:

storing a plurality of encryption keys in a storage medium and a read/write apparatus;

determining whether or not a match exists between an encryption key used by the storage medium and an encryption key used by the read/write apparatus, by comparing cipher data, which are encoded by the encryption key used by the storage medium and are transmitted from the storage medium, with cipher data encrypted by the encryption key used by the read/write apparatus;

determining, if no match exists, whether or not the encryption key used by the storage medium corresponds to an encryption key used in the past, by comparing the cipher data transmitted from the storage medium with the cipher data encrypted by the encryption key used by the read/write apparatus in the past; and

transmitting to the storage medium an update command for updating the encryption key used by the storage medium if the encryption key used by the storage medium corresponds to an encryption key used in the past;

wherein the storage medium updates the encryption key in response to the update command.

According to a fifth aspect of the present invention,

there is provided a station service system comprising:

- a boarding card corresponding to the storage medium as defined in the first aspect; and

- an automatic ticket examination machine equipped with the read/write apparatus as defined in any one of the first and second aspects;

wherein the read/write apparatus determines whether or not a match exists between an encryption key used by the boarding card and an encryption key used by the read/write apparatus, by comparing cipher data, which are encoded by the encryption key used by the boarding card and are transmitted from the boarding card, with cipher data encrypted by the encryption key used by the read/write apparatus;

- if no match exists, the read/write apparatus determines whether or not the encryption key used by the boarding card corresponds to an encryption key used in the past, by comparing the cipher data transmitted from the boarding card with the cipher data encrypted by the encryption key used by the read/write apparatus in the past;

- if the encryption key used by the boarding card corresponds to an encryption key used in the past, an update command for updating the encryption key used by the boarding card is transmitted to the boarding card; and the boarding card updates the encryption key in response to the update command.

According to a sixth aspect of the present invention, there is provided a station service system comprising:

- a boarding card corresponding to the storage medium as defined in the first aspect; and

- a card issuing machine equipped with the read/write

apparatus as defined in the second aspect, wherein the read/write apparatus rewrites a plurality of encryption keys stored in the boarding card at the time of issue of the boarding card.

According to a seventh aspect of the present invention, there is provided a card issuing machine comprising:

a boarding card corresponding to the storage medium as defined in the first aspect;

wherein the boarding card is issued by writing, into encryption key storage means of the boarding card, an encryption key that is currently used and a plurality of encryption keys to be used in the future, and by selecting the encryption key that is currently used by means of encryption key selection means.

The storage medium encrypts data to be sent to the read/write apparatus and decrypts data received from the same, through use of any one of the plurality of encryption keys. Even if one of the plurality of encryption keys is cracked, the security of the entire station service system is not compromised, which would otherwise occur in the common encryption key system. Further, the encryption key to be used is updated by means of a command issued by the read/write apparatus, as needed. Therefore, in contrast with the conventional system that randomly uses all the encryption keys, in the station service system according to the present invention, there is a much smaller chance that all the encryption keys will be intercepted and cracked.

In the storage medium according to the present invention, at least one of the plurality of encryption keys can be rewritten to a new encryption key by means of the read/write apparatus

before all the plurality of encryption keys stored in the storage medium are used through updating. Consequently, the encryption key can be updated to a new encryption key without limit.

The read/write apparatus determines whether or not an encryption key used by the storage medium corresponds to an encryption key used by the read/write apparatus in the past. If the encryption key is determined to correspond to a key used in the past, an update command is transmitted to the storage medium, so that the encryption key used by the storage medium can be updated. Accordingly, the encryption key of the storage medium can be matched with the most current encryption key that is currently used by the read/write apparatus.

In the read/write apparatus, the encryption key used by the storage medium is changed according to a command issued by a higher-level apparatus. The encryption key that is currently used can be changed to a new encryption key by means of a command issued by a higher-level apparatus, as needed; for example, periodically or in the event that the encryption key that is currently used is considered to be in danger of being cracked. Further, in combination with the foregoing operation, the encryption key used by the storage medium can also be matched with the new encryption key.

In the read/write apparatus according to the present invention, at least one of the plurality of encryption keys stored in the storage medium is rewritten, and hence the encryption keys can be rewritten to new encryption keys before all the encryption keys stored in the storage medium are sequentially updated and used, thereby enabling unlimited updating of the encryption key to a new encryption key.

In the card system according to the present invention, in the event that no match exists between the encryption key of the card and the encryption key of the read/write apparatus, so long as the encryption key of the card corresponds to an encryption key used in the past, the encryption key of the card is updated so as to match the encryption key of the read/write apparatus, thus enabling mutual authentication.

Under the encryption key utilization method according to the present invention, the read/write apparatus determines whether or not a match exists between an encryption key used by the storage medium and an encryption key used by the read/write apparatus, by comparing cipher data received from the storage medium with cipher data encrypted by the read/write apparatus. If no match exists, the read/write apparatus determines whether or not the encryption key used by the storage medium corresponds to an encryption key used by the read/write apparatus in the past. If the encryption key used by the boarding card corresponds to the encryption key used in the past, the encryption key of the storage medium is updated so that the encryption key of the storage medium can match the encryption key of the read/write apparatus.

In the station service system according to the present invention, a plurality of encryption keys for use in encryption processing effected between the boarding card and the read/write apparatus of the automatic ticket examination machine are stored in the boarding card and the read/write apparatus. The station service system involves little chance of security being compromised, which would otherwise occur in the common encryption key system when the common encryption key is cracked. Further, the encryption key to be used is updated

according to a command issued by the read/write apparatus, as needed. Therefore, in contrast with the conventional system that randomly uses all the encryption keys, the station service system involves little chance that all the encryption keys will be intercepted and cracked.

In the station service system according to the present invention, the card issuing machine rewrites the plurality of encryption keys stored in a boarding card at the time of issue of the boarding card, thereby enabling unlimited updating of the encryption key to a new encryption key.

The card issuing machine may be arranged not to recover expired boarding cards and reissue them as recycled boarding cards, but to issue new boarding cards. At the time of issue of the new boarding cards, the encryption key that is currently used and a plurality of encryption keys to be used in the future may be written into the cards without involvement of mutual authentication. Thus, the new boarding cards can be issued such that the encryption key that is currently used is selected.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram showing a station service system according to an embodiment of the present invention;

FIG. 2 is a perspective view showing an automatic ticket examination machine;

FIG. 3 is a block diagram showing a boarding card;

FIG. 4 is a table showing the contents of encryption storage memory of the boarding card;

FIG. 5 is a block diagram showing a read/write apparatus;

FIG. 6 is a table showing the expiration dates of encryption keys;

FIG. 7 is a table showing the contents of boarding card encryption key storage memory of the read/write apparatus;

FIG. 8 is a flowchart for describing the operation of the read/write apparatus of an automatic ticket examination machine;

FIG. 9 is a flowchart for describing an operation for mutual authentication; and

FIG. 10 is a flowchart for describing the operation of the read/write apparatus of a card issuing machine.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A preferred embodiment of the present invention will be described in detail hereinbelow by reference to the accompanying drawings.

FIG. 1 is a schematic diagram showing the overall configuration of a station service system to which the present invention is applied. In the drawing, reference numeral 7 designates a boarding card, such as a commuting pass, which is formed from a storage medium (e.g., a contactless communications IC card); 6 designates a read/write apparatus (a reader/writer) which establishes contactless communication with the boarding card 7; 1 designates an automatic ticket examination machine; 4 designates a card issuing apparatus equipped with the read/write apparatus 6; 5 designates a fare adjustment machine equipped with the read/write apparatus 6; and 25 designates a host computer for controlling all these elements. The plurality of automatic ticket examination machines 1 and the fare adjustment machines 5 are installed in the station precincts.

The boarding card 7 is issued by the card issuing machine

4, and data, such as a block of railroad track and an expiration date, are recorded on the boarding card 7. The thus-issued boarding card 7 is examined by the automatic ticket examination machine 1. Each of the card issuing machines 4 and the automatic ticket examination machines 1 is equipped with the read/write apparatus 6. The card issuing machines 4 and the automatic ticket examination machines 1 are higher in level than the read/write apparatus 6, and the host computer 25 is higher in level than the card issuing machines 4 and the automatic ticket examination machines 1. The automatic ticket examination machine 1 includes a CPU 26, interface circuits 27 and 28 between the host computer 25 and the read/write apparatus 6, memory 29, and a control circuit 30. The card issuing machine 4 comprises a CPU 31, interface circuits 32 and 33 between the host computer 25 and the read/write apparatus 6, memory 34, and a control console 35. Reference numerals, which will be used in the following description, are assigned to a block constituting the read/write apparatus 6.

A method of using the encryption key according to the present embodiment will be briefly described prior to description of the principal configuration of the system.

Authentication using an encryption key and communication are effected between the boarding card 7 and the read/write apparatus 6 in order to ensure security of the station service system. In the present embodiment, the following configuration is adopted in order to overcome the drawback of the conventional encryption processing system.

At the time of issue of the boarding card 7, a plurality of encryption keys to be used in the future are stored in the boarding card 7 beforehand. The boarding card 7 is set such

that a predetermined encryption key (for example, an encryption key to be used at the time of issue of the boarding card) from among the plurality of encryption keys is used. When an update command is issued from the read/write apparatus 6, the encryption key is updated to another encryption key designated by the update command, and the thus-updated encryption key is used.

A plurality of boarding cards 7 are sequentially issued over a long period of time, and hence the plurality of encryption keys recorded on the boarding cards 7 are sequentially switched to new encryption keys, as required. A plurality of encryption keys (for example, K1, K2, K3, K4, and K5) are recorded on an old boarding card 7 issued in the past, and another plurality of encryption keys (for example, K2, K3, K4, K5, and K6) are recorded on a new boarding card 7 issued later. Hence, common encryption keys (K2, K3, K4, and K5) exist between the two boarding cards 7. An old encryption key (K1), which is not recorded on the new boarding card 7, is recorded on the old boarding card 7. In contrast, a new encryption key (K6), which is to be used in the future and is not recorded on the old boarding card 7, is recorded on the new boarding card 7.

The plurality of encryption keys commonly recorded on all the boarding cards 7 are usable, and these encryption keys are used in sequence.

At least one old encryption key (e.g., K1), which was used in the past but is not used currently, and one encryption key (e.g., K2) that is currently used are stored in the read/write apparatus 6. The encryption key (e.g., K2) is used.

If the read/write apparatus 6 determines, on the basis of a response from the boarding card 7 through communication

with the boarding card 7, that the encryption key (e.g., K1) used by the boarding card 7 was used in the past but is not used currently, the read/write apparatus 6 issues an update command to the boarding card 7. In response to the update command, the boarding card 7 updates its encryption key (e.g., K1) to the encryption key (e.g., K2) that is currently used.

Consequently, the encryption keys used by the old boarding cards 7 issued in the past are updated and standardized to the encryption key (e.g., K2) that is currently used, through communication between the boarding cards 7 and the read/write apparatus 6.

In order to ensure the security of the station service system, the read/write apparatus 6 changes, periodically or when the encryption key that is currently used is considered to be in danger of being cracked, the encryption key (e.g., K2) that is currently used is changed to an encryption key (e.g., K3) to be used next, by means of a change command issued by a higher-level apparatus; i.e., the automatic ticket examination machine 1. The encryption key (K2) that has been used before this time is added to the read/write apparatus 6 as an old encryption key. Subsequently, the thus-changed encryption key (K3) is used. Consequently, at this point in time, the read/write apparatus 6 stores the plurality of encryption keys that were used in the past but are not used currently (e.g., K1 and K2) and the encryption key (e.g., K3) that is currently used.

When, through communication between the boarding card 7 and the read/write apparatus 6 whose encryption key is changed by means of a change command received from a higher-level apparatus, the boarding card 7 is found to use the encryption

key (e.g., K2) that was used in the past but is not used currently, the read/write apparatus 6 issues an update command to the boarding card 7. In response to the update command, the boarding card 7 updates its encryption key to the encryption key (e.g., K3) that is currently used.

Consequently, the encryption keys used by the old boarding cards 7 issued in the past are updated and standardized to the encryption key (e.g., K3) that is currently used, through communication between the boarding cards 7 and the read/write apparatus 6.

As mentioned above, the plurality of encryption keys are sequentially updated, and encryption processing is performed through use of the thus-updated encryption key. Therefore, even if one common encryption key is cracked, the security of the entire station service system will not be compromised, which would otherwise happen in the conventional common encryption key system. Further, the encryption key to be used is updated by means of an update command issued by the read/write apparatus 6, and hence there is little chance of all the encryption keys being intercepted and cracked, which would otherwise be caused in a case where all the encryption keys are used randomly.

The encryption key of the boarding card 7 is updated by means of an update command issued through communication between the boarding card 7 and the read/write apparatus 6, thus eliminating a necessity for changing the plurality of encryption keys of all the boarding cards 7 in unison.

The principal configuration of the boarding card 7 and the read/write apparatus 6 will now be described in detail.

FIG. 2 is a perspective external view showing the automatic ticket examination machine 1 equipped with the

read/write apparatus 6 according to the present embodiment. The automatic ticket examination machine 1 is equipped with a pair of ticket examination machine bodies 2 provided so as to face each other and to be spaced apart from each other with a passage 36 provided therebetween. An unillustrated wicket for allowing or hindering a passenger from walking through the passage 36 is disposed at one longitudinal end of the ticket examination machine body 2. Each of the ticket examination machine bodies 2 is equipped with the read/write apparatus 6, and an antenna coil 23 of the read/write apparatus 6 is provided so as to face the upper face of the ticket examination machine body 2.

When an antenna coil of the boarding card 7, such as a commuting pass, is situated within a communications area of the antenna coil 23, the antenna coil 23 can exchange data with the antenna coil of the boarding card 7 in a contactless manner. As shown in FIG. 2, a passenger carrying the boarding card 7 is required only to hold the boarding card 7 to the communications area formed in the ticket examination machine body 2 where the boarding card 7 establishes communication with the antenna coil 23 of the read/write apparatus 6, thus enabling data communication.

The read/write apparatus 6 communicates with the boarding card 7, and through such communication the automatic ticket examination machine 1, serving as a higher-level apparatus, determines whether the boarding card 7 is false or genuine, as well as boarding conditions. On the basis of determination results, the automatic ticket examination machine 1 controls the opening or closing action of the wicket.

As mentioned above, the plurality of encryption keys are

stored in the boarding card 7 according to the present embodiment. Data are encrypted or decrypted through use of any one of the plurality of encryption keys. The encryption key that is currently used is updated to another encryption key to be used next, by means of the update command issued by the read/write apparatus 6 of the automatic ticket examination machine 1. Further, at the time of issue of the boarding card 7, all the encryption keys stored in the boarding card 7 are rewritten by means of the read/write apparatus 6 of the card issuing machine 4. Not all the encryption keys stored in the boarding card 7, but only the expired encryption key may be rewritten to a new encryption key at the time of issue of the boarding card 7.

The boarding card 7 will now be described by reference to FIG. 3. The boarding card 7 comprises a CPU 8, program memory 9, data memory 10, encryption key storage memory 11, an encryption circuit 12, a modem power circuit 13, and the antenna coil 14.

The CPU 8 performs processing based on the command received from the read/write apparatus 6 by way of the antenna coil 14, through use of the program data stored in the program memory 9 and the working data stored in the data memory 10, and as well transmits data to the read/write apparatus 6.

The command transmitted to the boarding card 7 from the card read/write apparatus 6 comprises several types of commands; i.e., a polling command, an authentication command, a data read/write command, and a disable command. The CPU 8 receives such a command issued by the card read/write apparatus 6, by way of the antenna coil 14. The thus-received command is demodulated by the modem circuit 13 and is decrypted by means

of the decryption circuit 12. The thus-decrypted command is analyzed, and the CPU 8 performs processing in accordance with the thus-analyzed command.

As shown in FIG. 4, the read/write apparatus 6 of the card issuing machine 4 stores, in the encryption key storage memory 11 at the time of issue of the boarding card 7, a plurality of encryption keys (Encryption Key 1, Encryption Key 2, Encryption Key 3, ..., Encryption Key "n"), which are to be used by the boarding card 7 with respect to the read/write apparatus 6 of the automatic ticket examination machine 1. The encryption key storage memory 11 has such a hardware configuration as to completely prevent reading of the plurality of encryption keys from the outside. More specifically, the encryption key storage memory 11 is provided on an LSI chip, as is the CPU 8. Encryption keys are not output even if a test pin is connected to the LSI chip. Alternatively, the test terminal is removed from the LSI chip, and the LSI chip is arranged so as to permit only the CPU 8 provided within the LSI chip to read the data from the encryption key storage memory 11. The bus between the CPU 8 and the encryption key storage memory 11 is not exposed to the outside of the LSI chip in the form of a terminal. As a result, the encryption keys cannot be read from the outside of the LSI chip (or outside the circuit) at all.

The CPU 8 acts as encryption key selection means and selects a predetermined encryption key from Encryption Key 1, Encryption Key 2, Encryption Key 3, ..., Encryption Key "n" which are shown in FIG. 4 and stored in the encryption key storage memory 11, and the thus-selected encryption key is input to the encryption circuit 12. At the time of issue of a boarding card, Encryption Key 1, which is used at that point in time, and a

plurality of Encryption Keys 2, 3, ... to be sequentially used in the future are usually stored in the boarding card. Consequently, at the outset, Encryption Key 1 is set as an encryption key to be used.

Subsequently, if an update command is received from the read/write apparatus 6 of the automatic ticket examination machine 1, the CPU 8 acts as encryption key update means and updates the currently-set encryption key to another encryption key designated by the update command. The thus-updated encryption key is input to the encryption circuit 12.

The encryption circuit 12 encrypts or decrypts data through use of the thus-selected encryption key, and this encryption key is also used for mutual authentication between the boarding card 7 and the read/write apparatus 6 of the automatic ticket examination machine 1. As a matter of course, the boarding card 7 can receive a command for reading or writing data only after mutual authentication between the boarding card 7 and the read/write apparatus 6 has been effected.

The modem power circuit 13 modulates data to be sent to the read/write apparatus 6 of the automatic ticket examination machine 1, demodulates the data received from the read/write apparatus 6, and receives the transmission magnetic field developing in the read/write apparatus 6 by way of the antenna coil 14, to thereby generate power for the boarding card 7.

The read/write apparatus 6 according to the present embodiment is configured so as to authenticate and communicate with the boarding card 7, through use of an encryption key. The read/write apparatus 6 comprises encryption key storage means for storing a plurality of encryption keys; encryption key selection means for selecting any one from the plurality of

encryption keys stored in the encryption key storage means; encryption key awareness means for becoming aware of which one of the encryption keys was used in the past; command transmission means which transmits a command for updating the encryption key of the boarding card when the encryption key currently used by the boarding card is found to have been used in the past; and encryption key changing means for changing the encryption key used by the read/write apparatus in response to a command received from a higher-level apparatus.

The read/write apparatus 6 will be described hereinbelow by reference to FIG. 5. The read/write apparatus 6 comprises a CPU 15, program memory 16, data memory 17, an encryption circuit 18, boarding card encryption key storage memory 19, higher-level apparatus encryption key storage memory 20, a higher-level apparatus interface 21, a modem circuit 22, and the antenna coil 23. As mentioned above, a higher-level apparatus corresponds to the automatic ticket examination machine 1 or the card issuing machine 4.

The automatic ticket examination machine 1 controls, in addition to the read/write apparatus 6, a mechanism of actuating a wicket and communicates with the host computer 25 by way of the higher-level apparatus interface 21 of the read/write apparatus 6.

The read/write apparatus 6 effects mutual authentication with respect to a higher-level apparatus; i.e., the automatic ticket examination machine 1, at turn-on and ensures security of connection between the read/write apparatus 6 and the automatic ticket examination machine 1, thus performing, from then on, processing according to application software of the higher-level apparatus, such as the automatic ticket

examination machine 1.

In order to ensure the security of the station service system, in a case where the encryption key that is currently used reaches its expiration date or in the event that the encryption key that is currently used is considered to be in danger of being cracked, the host computer 25 sends a command for changing the encryption key that is currently used to the CPU 15 of the read/write apparatus 6 by way of a higher-level apparatus; i.e., the automatic ticket examination machine 1. By means of the command, the encryption key of the boarding card encryption key storage memory 19 is rewritten and changed, as will be described below. Subsequently, the read/write apparatus 6 performs processing with respect to the boarding card 7 through use of the thus-changed encryption key.

FIG. 6 is a table showing one example of the periods of use of encryption keys. In this example, if cracking of an encryption key does not occur and operations proceed correctly, the encryption key is changed every three months. Encryption Key 1 was used for three months from January 1st to March 31st, 1998. Encryption Key 2 is now used and will expire on July 30th, 1998 unless any accident occurs. Encryption Key 2 is to be changed to Encryption Key 3 on July 1st, 1998, and Encryption Key 3 is to be used thereafter.

The operation of the read/write apparatus 6 will now be described. The read/write apparatus 6 demodulates a command received from a higher-level apparatus, such as the automatic ticket examination machine 1, by way of the higher-level apparatus interface 21. The thus-demodulated command is analyzed by the CPU 15, and processing is performed according to the command. In a case where the higher-level apparatus

issues a command for reading data pertaining to the boarding card 7 stored in the data memory 10 of the boarding card 7; e.g., data pertaining to the expiration date and a block of railroad track specified by the commuting pass, the encryption circuit 18 encrypts a read command for reading data from the data memory 10 of the boarding card 7, through use of an encryption key selected from the boarding card encryption key storage memory 19. The thus-encrypted command is modulated by the modem circuit 22, and the modulated command is transmitted to the boarding card 7 by way of the antenna coil 23. Upon receipt of an answer signal from the boarding card 7 in response to the read command, the modem circuit 22 demodulates the answer signal, and the answer signal is decrypted by the encryption circuit 18, thereby acquiring the data regarding the boarding card 7. The data are encrypted by the encryption circuit 18, and the thus-encrypted data are transmitted to a higher-level apparatus by way of the higher-level apparatus interface 21. The higher-level apparatus; e.g., the automatic ticket examination machine 1, opens the wicket if the boarding card 7 is determined to be valid. If the boarding card 7 is determined to be invalid, the wicket will not open.

In addition to the conventional polling command, authentication command, and data read/write command, the command imparted to the boarding card 7 from the read/write apparatus 6 comprise commands for updating and rewriting the encryption key of the boarding card 7. In addition to the conventional commands; that is, a command for establishing communication with the boarding card 7, an authentication command, and a command for reading data from and writing data to the card read/write apparatus 6, the commands issued by a

higher-level apparatus, such as the automatic ticket examination machine 1 or the card issuing machine 4, comprise a command for updating the encryption key of the boarding card 7, a command for rewriting the encryption key of the boarding card 7, and a command for rewriting the encryption key of the card read/write apparatus 6.

As shown in FIG. 7, the encryption keys (old Encryption Key -m, ..., old Encryption Key -1) used by the boarding card 7 in the past and an encryption key that is currently used (current Encryption Key 0) are stored in the boarding card encryption key storage memory 19. The boarding card encryption key storage memory 19 is specifically designed for writing purposes and has such a hardware configuration as to prevent reading of data from the outside. Accordingly, unauthorized reading of an encryption key from the outside can be prevented. Since the hardware configuration has been described previously, repetition of its explanation will be omitted here. Of the plurality of encryption keys stored in the boarding card encryption key storage memory 19, the encryption key that is currently used is used for encrypting or decrypting the boarding card 7.

When a command for changing the encryption key that is currently used is issued by a higher-level apparatus, such as the automatic ticket examination machine 1, Encryption Key 0 shown in FIG. 7 and used currently is rewritten into an encryption key to be changed according to the change command. Encryption Key 0 that has been used so far is changed to old Encryption Key -1, and the encryption key that until now has been taken as old Encryption Key -1 is taken as old Encryption Key -2. Subsequent encryption keys are sequentially

reassigned numerals in the same manner. From then on, the thus-rewritten Encryption Key 0 that is currently used is used for processing. The oldest encryption key will become unnecessary at a point in time when none of the issued boarding cards 7 uses the encryption key, and hence the oldest encryption key is eliminated by means of overwriting.

Although in the present embodiment the encryption key used by the read/write apparatus 6 is arranged so that it can be rewritten by means of a change command issued by a higher-level apparatus, in another embodiment a plurality of encryption keys to be used later are stored even in the read/write apparatus 6 in advance such that an encryption key that is currently used is changed by means of an update command issued by a higher-level apparatus.

The encryption circuit 18 encrypts plaintext into a cipher text and decrypts a cipher text into plaintext. Further, the encryption circuit 18 is used for encrypting or decrypting a communications statement (command or response) to be transmitted to a higher-level apparatus or the boarding card 7, as well as for mutual authentication with respect to a higher-level apparatus and the boarding card 7. The boarding card 7 is usually arranged so as to receive another command after completion of mutual authentication with respect to the read/write apparatus 6.

The processing performed by the automatic ticket examination machine 1 will now be described by reference to a flowchart shown in FIG. 8.

If the boarding card 7 is not situated within the communications area where the boarding card 7 can communicate with the read/write apparatus 6 of the ticket examination

machine body 2, the read/write apparatus 6 transmits a polling command at a given cycle of about 10 milliseconds, by way of the antenna coil 23 (step n1). When the boarding card 7 approaches the communications area and sends an answer signal in response to the polling command (step n2), the read/write apparatus 6 and the boarding card 7 authenticate each other (step n3). Mutual authentication will be described later by reference to FIG. 9. If the read/write apparatus 6 and the boarding card 7 are authenticated, data are read from and written into the boarding card 7 (step n4). Finally, the read/write apparatus 6 prohibits the boarding card 7 that has been examined from answering a polling command transmitted to the next boarding card 7.

Mutual authentication will now be described by reference to FIG. 9.

Random data D_r are transmitted to the boarding card 7 from the read/write apparatus 6 (step n10). The boarding card 7 encrypts the random data D_r into cipher data D_r' , through use of the encryption key used by the boarding card 7, and the cipher data D_r' are transmitted to the read/write apparatus 6. The read/write apparatus 6 receives the cipher data D_r' (step n11) and encrypts the random data D_r through use of Encryption Key $K(0)$ that is currently used, thus producing cipher data $D_r'(0)$ (step n12). The read/write apparatus 6 compares the cipher data $D_r'(0)$ with the cipher data D_r' transmitted from the boarding card 7 (step n13). If a match exists between the cipher data $D_r'(0)$ and the cipher data D_r' , the boarding card 7 is determined to be valid. In contrast, if no match exists between them, the boarding card 7 is determined to be invalid or to use an old encryption key.

If the boarding card 7 is determined to be valid, random data Do are received from the boarding card 7 at this time (step n21). The random data Do are encrypted by means of Encryption Key K(0) that is currently used (step n22), and resultant cipher data Do' are transmitted to the boarding card 7 (step n23). When an answer signal is received from the boarding card 7 in response to transmission of the cipher data Do' (step n24), if the boarding card 7 and the read/write apparatus 6 are determined to be valid on the basis of the contents of the answer signal (step n25), mutual authentication is completed (step n26). In contrast, if the boarding card 7 and the read/write apparatus 6 are determined to be invalid, mutual authentication is determined to be no good (NG) (step n27).

If the boarding card 7 is not determined to be valid in step n13, the read/write apparatus 6 initializes the numeral assigned to the encryption key to 0 (i.e., $n=0$) (step n14). The number assigned to the encryption key is rewritten to the number assigned to the old encryption key ($n=n+1$) (step n15). Data are encrypted through use of Encryption Key K(n) assigned the thus-rewritten number (step n17), and a determination is made as to whether or not a match exists between the resultant cipher data and the cipher text returned from the boarding card 7 (step n18). The old encryption keys stored in the card read/write apparatus 6 are sequentially selected until a match is determined to exist (step n16). If a match exists between Dr' and Dr' (n) through use of the old encryption key assigned the number "n," the card read/write apparatus 6 determines that the encryption key used by the boarding card corresponds to Encryption Key K(n) assigned the old number. The card read/write apparatus 6 then issues an encryption key update

command to the boarding card 7 so that the encryption key assigned a pointer "n" of the encryption storage memory 11 is updated to the encryption key assigned pointer 0 (step n19), thereby updating the encryption key used by the boarding card 7 to Encryption Key K(0). Through the processing relating to steps subsequent to step n21, the boarding card 7 is determined to be valid.

Further, after updating of the encryption key of the boarding card 7, mutual authentication may be effected again through use of the new encryption key. If no match is found through use of all the individual old encryption keys stored in the card read/write apparatus 6, the boarding card 7 is determined to be invalid (step n20).

Processing of the read/write apparatus 6 of the card issuing machine 4 will now be described.

As shown in FIG. 10, in the card issuing machine 4 the read/write apparatus 6 performs the same processing operations as those shown in FIG. 8, with regard to the step of transmitting a polling signal, the step of receiving an answer signal, and the step of determining the card issuing machine 4 and the boarding card 7 to be valid through mutual authentication. After completion of mutual authentication shown in FIG. 10, an encryption key rewrite command is transmitted, and the data including the encryption key of the boarding card 7 are rewritten (step n4). At this time, the plurality of encryption keys stored in the encryption key storage memory 11 of the boarding card 7 are rewritten by means of an encryption key that is currently used and a plurality of encryption keys to be used later (step n5). As a result, at the outset the boarding card 7 selects and uses the encryption key that is currently used.

Later, the encryption key will be updated sequentially to the encryption keys in response to the update command.

If expired cards are not recovered and issued again but new boarding cards are issued, the only requirement is that an encryption key that is currently used and a plurality of encryption keys to be used later be written into the boarding cards without involvement of mutual authentication.

Although in the present embodiment the present invention is applied to a station service system, such as ticket examination machines, the present invention is not limited to such a system. The present invention can also be applied to an automatic fare collection system or other systems.

Although in the present embodiment the present invention is applied to contactless communication, the present invention may also be applied to contact communication.

As has been described above, the present invention yields the following advantageous results.

The storage medium encrypts data to be sent to the read/write apparatus and decrypts data received from the same, through use of any one of the plurality of encryption keys. Even if one of the plurality of encryption keys is cracked, the security of the entire station service system is not compromised, which would otherwise occur in the common encryption key system. Further, the encryption key to be used is updated by means of a command issued by the read/write apparatus, as needed. Therefore, in contrast with the conventional system that randomly uses all the encryption keys, in the station service system according to the present invention, there is a much smaller chance that all the encryption keys will be intercepted and cracked, thereby enhancing the security of the station

service system.

In the storage medium according to the present invention, at least one of the plurality of encryption keys can be rewritten to a new encryption key by means of the read/write apparatus before all the plurality of encryption keys stored in the storage medium are used through updating. Consequently, the encryption key can be updated to a new encryption key without limit, thus ensuring the security of the station service system without limit.

The read/write apparatus determines whether or not an encryption key used by the storage medium corresponds to an encryption key used by the read/write apparatus in the past. If the encryption key is determined to correspond to a key used in the past, an update command is transmitted to the storage medium, so that the encryption key used by the storage medium can be updated. Accordingly, the encryption key of the storage medium can be matched with the most current encryption key that is currently used by the read/write apparatus. Accordingly, changing of the encryption key used by the storage medium does not involve a difficult operation of recovering the storage mediums and changing in unison the encryption keys of the thus-recovered storage mediums. The encryption key of the storage medium is automatically changed through communication with the read/write apparatus while the storage medium is used.

In the read/write apparatus, the encryption key used by the storage medium is changed according to a command issued by a higher-level apparatus. The encryption key that is currently used can be changed to a new encryption key by means of a command issued by a higher-level apparatus, as needed; for example, periodically or in the event that the encryption key that is

currently used is considered to be in danger of being cracked. Further, in combination with the foregoing operation, the encryption key used by the storage medium can also be matched with the new encryption key.

In the read/write apparatus according to the present invention, at least one of the plurality of encryption keys stored in the storage medium is rewritten, and hence the encryption keys can be rewritten to new encryption keys before all the encryption keys stored in the storage medium are sequentially updated and used, thereby enabling unlimited updating of the encryption key to a new encryption key and ensuring the security of the station service system without limit.

In the card system according to the present invention, in the event that no match exists between the encryption key of the card and the encryption key of the read/write apparatus, so long as the encryption key of the card corresponds to an encryption key used in the past, the encryption key of the card is updated so as to match the encryption key of the read/write apparatus, thus enabling mutual authentication. Since the storage medium assumes the shape of a card, the storage medium can be suitably applied to various applications, such as an automatic fare collection system, thereby yielding the foregoing advantageous results noticeably.

Under the encryption key utilization method according to the present invention, the read/write apparatus determines whether or not a match exists between an encryption key used by the storage medium and an encryption key used by the read/write apparatus, by comparing cipher data received from the storage medium with cipher data encrypted by the read/write

apparatus. If no match exists, the read/write apparatus determines whether or not the encryption key used by the storage medium corresponds to an encryption key used by the read/write apparatus in the past. If the encryption key used by the boarding card corresponds to the encryption key used in the past, the encryption key of the storage medium is updated so that the encryption key of the storage medium can match the encryption key of the read/write apparatus.

The read/write apparatus of the storage medium stores a plurality of encryption keys. Even if one of the plurality of encryption keys is cracked, the security of the entire station service system is not compromised, which would otherwise occur in the common encryption key system. Further, the encryption key to be used is updated by means of a command issued by the read/write apparatus, as needed. Therefore, in contrast with the conventional system that randomly uses all the encryption keys, in the station service system according to the present invention, there is a much smaller chance that all the encryption keys will be intercepted and cracked. Further, the station service system does not involve a necessity of changing in unison the plurality of encryption keys stored in the storage medium.

In the station service system according to the present invention, a plurality of encryption keys for use in encryption processing effected between the boarding card and the read/write apparatus of the automatic ticket examination machine are stored in the boarding card and the read/write apparatus. The station service system involves little chance of security being compromised, which would otherwise occur in the common encryption key system when the common encryption key

is cracked. Further, the encryption key to be used is updated according to a command issued by the read/write apparatus, as needed. Therefore, in contrast with the conventional system that randomly uses all the encryption keys, the station service system involves little chance that all the encryption keys will be intercepted and cracked. Further, the station service system does not involve a necessity of changing in unison the plurality of encryption keys stored in the storage medium.

In the station service system according to the present invention, the card issuing machine rewrites the plurality of encryption keys stored in a boarding card at the time of issue of the boarding card, thereby enabling unlimited updating of the encryption key to a new encryption key.

The card issuing machine may be arranged not to recover expired boarding cards and reissue them as recycled boarding cards, but to issue new boarding cards. At the time of issue of the new boarding cards, the encryption key that is currently used and a plurality of encryption keys to be used in the future may be written into the cards without involvement of mutual authentication. Thus, the new boarding cards can be issued such that the encryption key that is currently used is selected.

WHAT IS CLAIMED IS:

1. A storage medium configured so as to effect authentication and establish communication with a read/write apparatus through use of an encryption key, said storage medium comprising:

encryption key storage means for storing a plurality of encryption keys;

encryption key selection means for selecting any one from among the plurality of encryption keys stored in the encryption key storage means; and

encryption key update means for updating the thus-selected encryption key according to a command transmitted from the read/write apparatus.

2. The storage medium as defined in claim 1, wherein the read/write apparatus rewrites at least one of the plurality of encryption keys stored in the encryption key storage means.

3. A read/write apparatus which effect authentication and establish communication with a storage medium through use of an encryption key; said apparatus comprising:

encryption key storage means for storing a plurality of encryption keys;

encryption key selection means for selecting any one from among the plurality of encryption keys stored in the encryption key storage means;

encryption key awareness means for becoming aware of, on the basis of a response from the storage medium, whether or not the encryption key that is currently used by the storage medium corresponds to an encryption key used in the past by the read/write apparatus; and

encryption key update command transmission means which



transmits a command for updating the encryption key of the storage medium when the encryption key currently used by the storage medium corresponds to an encryption key used in the past.

4. The read/write apparatus as defined in claim 3, further comprising encryption key changing means for changing the encryption key to be used by the read/write apparatus, in response to a command issued by a higher-level apparatus.

5. The read/write apparatus as defined in claim 3, wherein the storage medium rewrites at least one of the plurality of encryption keys stored.

6. A card system comprising:
a card corresponding to the storage medium as defined in claim 1 or 2; and
the read/write apparatus as defined in any one of claims 3 to 5, wherein

if the encryption key currently used by the card corresponds to an encryption key used by the read/write apparatus in the past, the encryption key of the card is updated, and then mutual authentication between the card and the read/write apparatus is effected through use of the thus-updated encryption key.

7. An encryption key utilization method comprising the steps of:

storing a plurality of encryption keys in a storage medium and a read/write apparatus;

determining whether or not a match exists between an encryption key used by the storage medium and an encryption key used by the read/write apparatus, by comparing cipher data, which are encoded by the encryption key used by the storage



medium and are transmitted from the storage medium, with cipher data encrypted by the encryption key used by the read/write apparatus;

determining, if no match exists, whether or not the encryption key used by the storage medium corresponds to an encryption key used in the past, by comparing the cipher data transmitted from the storage medium with the cipher data encrypted by the encryption key used by the read/write apparatus in the past;

transmitting to the storage medium an update command for updating the encryption key used by the storage medium if the encryption key used by the storage medium corresponds to an encryption key used in the past; and

the storage medium updates the encryption key in response to the update command.

8. A station service system comprising:

a boarding card corresponding to the storage medium as defined in claim 1 or 2; and

an automatic ticket examination machine equipped with the read/write apparatus as defined in claim 3 or 4, wherein

the read/write apparatus determines whether or not a match exists between an encryption key used by the boarding card and an encryption key used by the read/write apparatus, by comparing cipher data, which are encoded by the encryption key used by the boarding card and are transmitted from the boarding card, with cipher data encrypted by the encryption key used by the read/write apparatus;

if no match exists, the read/write apparatus determines whether or not the encryption key used by the boarding card corresponds to an encryption key used in the past, by comparing



the cipher data transmitted from the boarding card with the cipher data encrypted by the encryption key used by the read/write apparatus in the past;

if the encryption key used by the boarding card corresponds to an encryption key used in the past, an update command for updating the encryption key used by the boarding card is transmitted to the boarding card; and the boarding card updates the encryption key in response to the update command.

9. A station service system comprising:

a boarding card corresponding to the storage medium as defined in claim 1 or 2; and

a card issuing machine equipped with the read/write apparatus as defined in claim 5, wherein the read/write apparatus rewrites a plurality of encryption keys stored in the boarding card at the time of issue of the boarding card.

10. A card issuing machine comprising:

a boarding card corresponding to the storage medium as defined in claim 1 or 2,

wherein the boarding card is issued by writing, into encryption key storage means of the boarding card, an encryption key that is currently used and a plurality of encryption keys to be used in the future, and by selecting the encryption key that is currently used by means of encryption key selection means.

