MEMORY DEVICE AND METHOD

CROSS-REFERENCE TO RELATED APPLICATION

This application is based upon and claims the benefit of priority from Japanese Patent Application No. 2015-140557; filed July 14, 2015; the entire contents of which are incorporated herein by reference.

FIELD

Embodiments described herein relate generally to a memory device and a method.

BACKGROUND

These days, a memory device which can be coupled to a terminal device is provided. Update processing of, for example, firmware is performed between a delivery serer and the terminal device, using a communication network such as Internet.

An example of the related art includes JP-A-2010-152877.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a configuration of a memory device according to a first embodiment.

FIG. 2 is a diagram illustrating system configured by a memory device, terminal device, and a delivery server according to the first embodiment.

FIG. 3 is a sequence diagram illustrating a firmware update operation according to the first embodiment.

FIG. 4 is a diagram illustrating a system which is configured by a memory device, terminal device, and a delivery server according to a second embodiment.

FIG. 5 is a flowchart illustrating an example of an operation of the delivery server according to the second embodiment.

FIG. 6 is a block diagram illustrating a configuration of a memory device according to a third embodiment.

FIG. 7 is a diagram illustrating system configured by the memory device, a terminal device, and a delivery server according to the third embodiment.

FIG. 8 is a sequence diagram illustrating a firmware update operation according to the third embodiment.

FIG. 9 is a block diagram illustrating a configuration of a memory device according to a fourth embodiment.

FIG. 10 is a sequence diagram illustrating a patch application operation according to the fourth embodiment.

DETAILED DESCRIPTION

[0004]Exemplary embodiments described herein increase reliability of a terminal device in which a memory device is embedded.

[0005]In general, according to one embodiment, a memory device includes a receiving unit that receives processing data and first authentication information which are transmitted from a server through an external apparatus; a memory unit that stores the processing data; a generation unit that generates a first signature, based on a first key which is stored in advance and the received first authentication information; and a transmission unit that transmits response data including the first signature and the first authentication information to the server through the external apparatus.

[0007]Embodiments will be hereinafter described with reference to the accompanying drawings.

[0008]In the present specification, an example of a plurality of expressions is used for some elements. The example of the expressions is just illustrative, and it does not deny that the elements are expressed differently. In addition, elements in which a plurality of expressions are not used may also be expressed differently.

[0009]In addition, the drawings are schematic, and a relationship between a thickness and a plan dimension, a ratio of the thickness of each layer, or the like may be different from actual ones. In addition, a portion having a dimensional relationship or a ratio different from each other may be included in the drawings.

First Embodiment

[0010]FIG. 1 is a block diagram illustrating an example of a configuration of a memory device 1 according to a first embodiment. The memory device 1 is, for example, a hard disk drive (HDD), but the embodiment is not limited to this, and the memory device 1 may be a solid state drive (SSD) or a combination of the HDD and the SSD.

[0011]The memory device 1 includes, for example, a data transmission unit 10, a data receiving unit 20, an encryption processing unit 30, a firmware storage area 40, a response data storage area 50, a digital signature generation unit 60, and a secret key storage area 70. In addition, the encryption processing unit 30 includes an encryption calculation unit 31 and a random number generation unit 32.

[0012]FIG. 2 illustrates a system which is configured by a terminal device 100 that includes the memory device 1, and a delivery server 200 that transmits data to the terminal device 100. The terminal device 100 and the delivery server 200 are coupled to each other by an internet protocol (IP) network 300. Meanwhile, the terminal device 100 and the delivery server 200 may be coupled to each other by other methods using, such as a 3G network, a 4G network, a long term evolution network (LTE), or a TV broadcasting wave. In addition, in the present embodiment, the delivery server 200 updates firmware of the terminal device 100.

[0013]As described above, the memory device 1 is embedded in the terminal device 100. The terminal device 100 is a terminal such as a point of sale (POS) or multifunction peripheral (MFP), but is not limited to this, and may be a television, a recorder, a personal computer (PC), or the like. Meanwhile, the terminal device 100 can be referred to as an external apparatus of the memory device 1.

[0014]For example, if performing update of the firmware of the terminal device 100, the delivery server 200 deliveries update data to the terminal device 100 through an IP network 300, together with firmware update requests.

[0015]In addition, if update of the terminal device 100 is completed, the delivery server 200 receives response data from the terminal device 100, which will be described later.

[0016]Returning to FIG. 1, the data transmission unit 10 transmits data to the outside of the memory device 1. In the first embodiment, for example, the data transmission unit 10 transmits response data to the delivery server 200 through the terminal device 100, in response to data which is transmitted from the delivery server 200 through the terminal device 100.

[0017]The data receiving unit 20 receives data from the outside of the memory device 1. In the present embodiment, for example, when the data receiving unit 20 is updated, the data receiving unit 20 receives update data from the delivery server 200 through the terminal device 100.

[0018]Meanwhile, for the sake of convenient description, the data transmission unit 10 and the data receiving unit 20 are exemplified in a separated state, but for example, a data transmission and receiving unit or an interface unit in which the data transmission unit 10 and the data receiving unit 20 are integrally configured, may be provided.

[0019]The encryption processing unit 30 performs encryption processing of the data which is handled by the memory device 1. For example, the encryption calculation unit 31 encrypts a digital signature which is added to the data that is received by the memory device 1 as authentication information, using a secret key that is stored in the secret key storage area 70. The random number generation unit 32 generates a random number for judging validity of data that is received by the data receiving unit 20, for example, for each preset time.

[0020]Firmware data of the terminal device 100 and update data delivered from the delivery server 200 are stored in the firmware storage area 40.

[0021]Response data that is transmitted to the delivery server 200 and is generated in the memory device 1 is temporarily stored in the response data storage area 50.

[0022]The digital signature generation unit 60 generates a digital signature of challenge data that is transmitted from the delivery server 200. Meanwhile, the digital signature is stored in the response data storage area 50 as response data.

[0023]A secret key that is used when the digital signature generation unit 60 generates a digital signature is stored in the secret key storage area 70.

[0024]FIG. 3 is a sequence diagram illustrating a firmware update operation according to the first embodiment. The firmware update operation of the terminal device 100 will be hereinafter described with reference to FIG. 3.

[0025]If it is necessary to update the firmware of the terminal device 100, the delivery server 200 issues a firmware update request for the terminal device 100 (S1.1). At this time, the delivery server 200 transmits the update data to the terminal device 100, at the same time as when the firmware update request is issued.

[0026]Meanwhile, it may be configured such that the delivery server 200 initially transmits only the firmware update request to the terminal device 100, receives response after confirming whether or not the terminal device 100 is in a updatable state, and thereafter transmits the update data to the terminal device 100.

[0027]Hereinafter, description will be made with an assumption that the “firmware update request” includes the update data. Meanwhile, in the present embodiment, the “update data” includes program data of a new firmware and challenge data.

[0028]The terminal device 100 transmits the firmware update request that is received from the delivery server 200 to the memory device 1 using, for example, a dedicated command (A1.2). The update data that is received through the data receiving unit 20 of the memory device 1 is written to the firmware storage area 40 of the memory device 1. That is, program data of a new firmware is stored in the firmware storage area 40 (S1.3).

[0029]Subsequently, in the memory device 1, the digital signature generation unit 60 generates a digital signature of the challenge data that is included in the update data, using a secret key that is stored in advance in the secret key storage area 70 (S1.4). The generated digital signature is stored in the response data storage area 50 as the response data in parallel with the challenge data (S1.5). The memory device 1 completes processing according to the firmware update request, and returns a command to the terminal device 100 through the data transmission unit 10 (S1.6).

[0030]If receiving the command from the memory device 1, the terminal device 100 issues a response data request to the memory device 1 (S1.7).

[0031]If receiving the response data request through the data receiving unit 20, the memory device 1 acquires the response data from the response data storage area 50 (S1.8), and transmits the response data (command) to the terminal device 100 through the data transmission unit 10 (S1.9).

[0032]If receiving the command, the terminal device 100 issues update completion notification to the delivery server 200 together with the response data (S1.10). By performing authentication of the digital signature of the received response data, the delivery server 200 can confirm that the firmware update of the terminal device 100 is correctly completed.

[0033]Here, challenge and response authentication that is performed between the delivery server 200 and the terminal device 100 will be described. The delivery server 200 issues a firmware update request for the terminal device 100. The terminal device 100 receives the challenge data together with the firmware update request. Thereafter, if finally receiving the response data from the terminal device 100, the delivery server 200 completes the challenge and response authentication, and determines that the firmware update is correctly performed.

[0034]However, for example, if unauthorized access of the terminal device 100 is performed from the outside, there is a possibility that the firmware update completion is spoofed by faking authentication. More specifically, problems can be made in which the terminal device 100 returns the response data to the delivery server 200, but a new firmware is not transmitted to the memory device 1 and actually update of the firmware is not performed.

[0035]In addition, even if the terminal device 100 is infected with virus or the like, the same problems as described above can be made. Furthermore, the update of the firmware can also be blocked by the terminal device 100.

[0036]Thus, in the present embodiment, the challenge and response authentication is performed between the delivery server 200 and the memory device 1.

[0037]In general, the memory device 1 is configured by a dedicated hardware which is independent from the terminal device 100. For this reason, unauthorized access or alteration from the outside can be prevented, compared to the terminal device 100. By performing the channel and response authentication between the memory device 1 and the delivery server 200, it is possible to confirm that the firmware update is correctly completed.

[0038]In addition, if the terminal device 100 receives an unauthorized access thereby performing an unauthorized operation, the delivery server 200 or the memory device 1 can detect that the firmware update is not correctly performed. For this reason, it is possible to rapidly perform countermeasure, such as disconnection of the terminal device 100 from the IP network 300, or initialization caused by a maintenance person. Furthermore, it is also possible to perform countermeasure such as no start of the firmware which can be unauthorized-accessed, when restarting.

Second Embodiment

[0039]FIG. 4 illustrates a system which is configured by the terminal device 100 in which the memory device 1 is embedded, and the delivery server 200 according to a second embodiment. In addition, FIG. 5 is a flowchart illustrating an example of an operation of the delivery server 200 according to the second embodiment. Meanwhile, in the description of the present embodiment, the same symbols or reference numerals will be attached to the same configuration elements as in the first embodiment, and detailed description thereof will be omitted.

[0040]In the present embodiment, the delivery server 200 includes a timer 201, as illustrated in FIG. 4. The delivery server 200 starts the timer 201 according to issue of a firmware update request for the terminal device 100. With this configuration, the delivery server 200 can judge that firmware update is not correctly performed, if response data (update completion notification) is not transmitted from the terminal device 100 within a predetermined time which is set in advance.

[0041]Meanwhile, the “predetermined time” may be a value which is set by an administrator of the delivery server, and may be appropriately modified according to a size of the update data (particularly, new firmware) which is transmitted together with the firmware update request, complexity of firmware update processing, or the like.

[0042]In general, it is preferable that the predetermined time which is set by the timer 201 and in a case in which the update data is large is set longer than that in a case in which the update data is small. This is due to the fact that it takes more time to perform the firmware update than a case in which the size of the update data is large.

[0043]In addition, a predetermined time that is measured by the timer 201 may be configured to be changed according to content of the firmware update processing. For example, a case is taken into account in which the content of the firmware update means that the update data is added (that is written) to the firmware storage area 40 of the memory device 1. In this case, time required for updating the firmware is shorter than that when the content of the firmware update means that the firmware which is stored in advance in the firmware storage area 40 is changed (that is rewritten).

[0044]For example, in a case in which the memory device 1 is an HDD, if the existing data is changed, new data overwrites the existing data. For this reason, time required for writing the data does not change so much, compared to a case in which the data is written to an empty area.

[0045]Meanwhile, in a case in which the memory device 1 is an SSD, when the existing data is changed to new data, it is necessary to erase the data that is no longer required, among the existing data. In general, a flash memory that is used for the SSD takes more time when erasing the data, compared to when writing the data.

[0046]For example, for the firmware update, it is necessary to erase the firmware that is stored in the firmware storage area 40 prior to the update, and to store new update data in the firmware storage area 40. For this reason, it takes more time compared to when the data is written to an empty area.

[0047]In general, writing speed to the SSD is faster than that to the HDD. Thus, a configuration in which the “predetermined time” described above is changeable according to the type of the memory device 1 may be provided.

[0048]FIG. 5 illustrates an example of an operation of the delivery server 200 according to the present embodiment. If it is necessary to update the firmware of the terminal device 100, the delivery server 200 issues a firmware update request for the terminal device 100 (S2.1).

[0049]The delivery server 200 activates the timer 201 according to the issue of the firmware update request, and starts measurement of elapsed time t (S2.2). Meanwhile, the sequence of the firmware update request and the start of the timer 201 may be reversed. It is preferable that the time between S2.1 and S2.2 is short in either case.

[0050]Thereafter, it is confirmed whether or not a predetermined time T has passed, after the firmware update request is issued (S2.3), and if t³T is satisfied, it is confirmed whether or not there is a response from the terminal device 100 and the memory device 1 (S2.4).

[0051]In S2.4, if not receiving a response from the terminal device 100 and the memory device 1 (No of S2.4), the delivery server 200 may estimate that the firmware update fails.

[0052]In addition, in S2.4, if receiving a response from the terminal device 100 and the memory device 1 (Yes of S2.4), the delivery server 200 performs response authentication in the same manner as in the first embodiment (S2.5), and determines that the update is correctly performed from the authentication result.

[0053]If the response authentication is successful (Yes of S2.5), the delivery server 200 recognizes that the firmware update of the terminal device 100 is successful. Meanwhile, if the response authentication fails (No of S2.5), the delivery server 200 recognizes that the firmware update of the terminal device 100 fails.

[0054]In the configuration described in the present embodiment, the delivery server 200 can recognize not only from the result of the challenge and response authentication described in the first embodiment, but also in a case in which the response is not returned from the terminal device 100 and the memory device 1 within the predetermined time.

[0055]By the configuration described above, for example, if the response data is not returned to the delivery server even after the elapse of the predetermined time, it is estimated that it is due to that the terminal device 100 is infected with virus or the like, or due to unauthorized access, alteration, or the like from the outside. As a result, it is possible to rapidly perform countermeasure, such as disconnection from the IP network 300, or initialization performed by a maintenance person.

[0056]Meanwhile, the timer 201 according to the present embodiment is not need to be newly provided in the delivery server 200 described in the first embodiment, and if a hardware configuration or a function included in the delivery server 200 contains a clock function, that may be used as the timer 201 according to the present embodiment.

Third Embodiment

[0057] FIG. 6 is a block diagram illustrating an example of a configuration of a memory device 1 according to a third embodiment. In addition, FIG. 7 illustrates a system configured by a terminal device 100 in which the memory device 1 according to the third embodiment is embedded and a delivery server 200. Meanwhile, in the description of the third embodiment, the same symbols or reference numerals will be attached to the same configuration elements as those of the first embodiment and the second embodiment, and description thereof will be omitted.

[0058]As described in FIG. 6, the memory device 1 includes a public key storage area 80, and public keys of the delivery server 200 are stored in the public key storage area 80.

[0059]In addition, the memory device 1 includes an authentication unit 35. The authentication unit 35 performs authentication using the public keys stored in the public key storage area 80.

[0060]Furthermore, as illustrated in FIG. 7, the delivery server 200 includes a secret key storage area 202 and a digital signature generating unit 203. Secret keys of the delivery server 200 are stored in the secret key storage area 202. The digital signature generating unit 203 generates a digital signature for challenge data.

[0061]FIG. 8 is a sequence diagram illustrating a firmware update operation according to the third embodiment. The firmware update operation of the terminal device 100 according to the third embodiment will be hereinafter described with reference to FIG. 8.

[0062]If it is necessary to update the firmware of the terminal device 100, the delivery server 200 issues a firmware update request for the terminal device 100 (S3.1). At this time, the delivery server 200 transmits update data to the terminal device 100 at the same time when the firmware update request is issued. Meanwhile, in the third embodiment, the update data includes program data of a new firmware, and first challenge data.

[0063]The terminal device 100 transmits the firmware update request received from the delivery server to the memory device 1 using, for example, a dedicated command (S3.2). The update data which is received through the data receiving unit 20 of the memory device 1 is written to the firmware storage area 40 of the memory device 1, and the program data of the new firmware is stored in the firmware storage area 40 (S3.3).

[0064]Subsequently, in the memory device 1, the digital signature generation unit 60 generates a first digital signature of the first challenge data which is included in the update data by using the secret keys that is stored in advance in the secret key storage area 70 (S3.4). The generated first digital signature is stored in the response data storage area 50 as first response data in parallel with the first challenge data (S3.5). The memory device 1 completes processing according to the firmware update request, and issues a command to the terminal device 100 through the data transmission unit 10 (S3.6).

[0065]If receiving a command from the memory device 1, the terminal device 100 issues a first response data request to the memory device 1 (S3.7).

[0066]If receiving the first response data request through the data receiving unit 20, the memory device 1 acquires the first response data from the response data storage area 50 (S3.8), and in parallel with this, generates second challenge data (S3.9). The memory device 1 transmits the first response data to the terminal device 100 through the data transmission unit 10 (S3.10).

[0067]In the third embodiment, the memory device 1 transmits not only the first digital signature but also the second challenge data, to the terminal device 100. Thus, the first response data that the terminal device 100 receives from the memory device 1, includes the first digital signature of the first challenge data, and the second challenge data.

[0068]If receiving the command from the memory device 1, the terminal device 100 issues a second response data request to the delivery server 200 (S3.11). At this time, the first response data is transmitted from the terminal device 100 to the delivery server 200.

[0069]If the delivery server 200 receives the second response data request from the terminal device 100, the digital signature generating unit 203 of the delivery server 200 generates a second digital signature of the second challenge data which is included in the first response data, using the secret keys which is stored in advance in the secret key storage area 202 of the delivery server 200 (S3.12). The generated second digital signature is transmitted to the terminal device 100 as second response data (S3.13).

[0070]The terminal device 100 which receives the second response data transmits a dedicated command to the memory device 1 (S3.14).

[0071]The memory device 1 which receives the second digital signature from the terminal device 100 performs authentication of the second response data which is transmitted according to the command. Specifically, as the authentication unit 35 verifies the second response data using the public keys of the delivery server 200, the memory device 1 can confirm that the authentication which is performed in the delivery server 200 is successful.

[0072]As described above, in the third embodiment, the challenge and response authentication is mutually performed between the delivery server 200 and the memory device 1 through the terminal device 100. Meanwhile, the present embodiment has a configuration in which, when returning the response with respect to the first challenge data that is received from the delivery server 200, the memory device 1 transmits the second challenge data to the delivery server 200, and receives the response with respect to the second challenge data from the delivery server 200.

[0073]In other words, in the present embodiment, the delivery server 200 and the memory device 1 bidirectionally perform the challenge and response authentication.

[0074]Thus, as receiving the response with respect to the second challenge data from the delivery server 200, the memory device 1 can confirm that the firmware update of the terminal device 100 is correctly performed.

[0075]Furthermore, if there is a problem in the result of the challenge and response authentication, for example, information indicating that the firmware update fails is output to the terminal device 100, and thereby a user which uses the terminal device 100 can know that the firmware update fails. Meanwhile, at this time, it is possible to notify the user of the failure of the firmware update, using a display which is included in the terminal device 100, for example.

[0076]In addition, if there is a problem in the result of the challenge and response authentication, the terminal device 100 may be configured (disabled) to not be able to perform the firmware which is stored in the memory device 1, when the terminal device 100 is activated thereafter.

Fourth Embodiment

[0077]The challenge and response authentication of the delivery server 200 and the memory device 1 which is described in the first embodiment to the third embodiment is not needed to be used for the firmware update.

[0078]The fourth embodiment may have a configuration in which the delivery server 200 confirms whether or not chip application to an OS which is executed by the terminal device 100 is correctly performed, through the challenge and response authentication of the memory device 1.

[0079]FIG. 9 is a block diagram illustrating an example of a configuration of a memory device 1 according to a fourth embodiment. FIG. 10 is a sequence diagram illustrating a patch application operation according to the fourth embodiment. The patch application operation of the terminal device 100 will be hereinafter described with reference to FIG. 9 and FIG. 10.

[0080]The delivery server 200 issues a patch application request with respect to the terminal device 100 as necessary (S4.1). Meanwhile, the “patch application request” includes patch data that is used for patch application, and challenge data.

[0081]The terminal device 100 transmits the patch application request which is received from 200 to the memory device 1, using, for example, a dedicated command (S4.2). The patch data that the memory device 1 receives is written to a patch data storage area 90 of the memory device 1 (S4.3).

[0082]Subsequently, in the memory device 1, the digital signature generation unit 60 generates a digital signature of the challenge data, using the secret keys which are stored in advance (S4.4). The generated digital signature is stored in the response data storage area 50 as response data in parallel with the challenge data (S4.5). The memory device 1 completes processing according to the patch application request, and returns the command to the terminal device 100 (S4.6).

[0083]If receiving a command from the memory device 1, the terminal device 100 issues a response data request to the memory device 1 (S4.7).

[0084]If receiving the response data request, the memory device 1 acquires response data (S4.8), and transmits the response data (command) to the terminal device 100 (S4.9).

[0085]If receiving the command from the memory device 1, the terminal device 100 issues a patch application completion notification to the delivery server 200 together with the response data (S4.10). By performing authentication of the digital signature of the received response data, the delivery server 200 can confirm that the patch application of the terminal device 100 is correctly completed.

[0086]Meanwhile, as described in the second embodiment, the present embodiment may have a configuration in which, when the delivery server 200 starts the patch application, the timer is set, and if the response data is not returned from the memory device 1 within a predetermined time, it is possible to confirm that the patch application is correctly executed.

[0087]In addition, as described in the third embodiment, the present embodiment has a configuration in which, when the memory device 1 returns the response data, new challenge data which is arbitrarily generated by the memory device 1 is transmitted to the delivery server 200 together with the response data, and new response data with respect to the new challenge data is transmitted to the memory device 1. Thereby, the delivery server 200 and the memory device 1 may mutually perform the challenge and response authentication.

[0088]As described above, in the present embodiment, the delivery server 200 can confirm that the patch application of the terminal device 100 is correctly performed.

[0089]In addition, if the terminal device 100 receives unauthorized access and performs unauthorized operation, the delivery server 200 or the memory device 1 can detect a situation in which the patch application is not correctly performed, and thereby it is possible to rapidly perform countermeasure, such as disconnection from the IP network 300, or initialization performed by a maintenance person.

[0090]Meanwhile, in the first embodiment to the fourth embodiment, the delivery server 200 transmits the program data of the firmware or the patch data to the memory device 1 through the terminal device 100, but data to be handled is not limited to this, and, for example, may be parameter data or the like.

[0091]In addition, in the first embodiment to the fourth embodiment, various commands (command, response) are exchanged between the delivery server 200, the terminal device 100, and the memory device 1, through an I/F. However, a response command may be a static signal using other coupling terminals, not the I/F.

[0092]Furthermore, the memory device 1 may have a configuration in which the firmware is not rewritten immediately after the program data of the firmware is received, but, the firmware is temporarily stored in a volatile memory such as a RAM, and is updated after the challenge and response authentication is completed.

[0093]While certain embodiments have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions. Indeed, the novel embodiments described herein may be embodied in a variety of other forms; furthermore, various omissions, substitutions and changes in the form of the embodiments described herein may be made without departing from the spirit of the inventions. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the inventions.

WHAT IS CLAIMED IS:

1. A memory device comprising:

a receiving unit that receives processing data and first authentication information which are transmitted from a server through an external apparatus;

a memory unit that stores the processing data;

a generation unit that generates a first signature, based on a first key which is stored in advance and the received first authentication information; and

a transmission unit that transmits response data including the first signature and the first authentication information to the server through the external apparatus.

2. The device according to Claim 1, wherein the response data is temporarily retained in the memory unit, and is transmitted to the server in response to a command from the external apparatus.

3. The device according to Claim 1 or 2,

wherein the response data further includes second authentication information for authenticating the server, and

wherein the device further comprises an authentication unit that performs authentication, based on the second authentication information, and a second signature which corresponds to the second authentication information and is received from the server through the external apparatus.

4. The device according to Claim 3, wherein, if the authentication fails, information indicating failure of the authentication is output to the external apparatus.

5. The device according to any one of Claims 1 to 4, wherein the processing data includes program data of firmware of the external apparatus.

6. An authenticating method of a memory device including a memory unit, the method comprising:

receiving processing data and first authentication information which are transmitted from a server through an external apparatus;

generating a signature, based on a key which is stored in advance and the first authentication information; and

transmitting response data including the signature and the first authentication information to the server through the external apparatus.

7. An authenticating method of a server that delivers processing data, the method comprising:

transmitting the processing data and first authentication information to a memory device through an external apparatus;

receiving response data including a first signature and the first authentication information, based on the first authentication information, through the external apparatus; and

confirming whether or not authentication of the memory device is successful, with reference to the response data.

8. An authenticating method of a terminal device which is coupled to a memory device, the method comprising:

receiving processing data and first authentication information which are transmitted from a server;

transmitting the processing data and the first authentication information to the memory device;

receiving response data including first signature and the first authentication information, based on the first authentication information, from the memory device; and

transmitting the response data to the server.

ABSTRACT

According to one embodiment, a memory device includes a receiving unit that receives processing data and first authentication information which are transmitted from a server through an external apparatus; a memory unit that stores the processing data; a generation unit that generates a first signature, based on a first key which is stored in advance and the received first authentication information; and a transmission unit that transmits response data including the first signature and the first authentication information to the server through the external apparatus.

Drawings

FIG. 1

1: MEMORY DEVICE

10: DATA TRANSMISSION UNIT

30: ENCRYPTION PROCESSING UNIT

31: ENCRYPTION CALCULATION UNIT

32: RANDOM NUMBER GENERATION UNIT

70: SECRET KEY STORAGE AREA

20: DATA RECEIVING UNIT

50: RESPONSE DATA STORAGE AREA

60: DIGITAL SIGNATURE GENERATION UNIT

40: FIRMWARE STORAGE AREA

FIG. 2

200: DELIVERY SERVER

300: INTERNET PROTOCOL NETWORK

100: TERMINAL DEVICE

1: MEMORY DEVICE

FIG. 3

200: DELIVERY SERVER

100: TERMINAL DEVICE

1: MEMORY DEVICE

S1.1: FIRMWARE UPDATE REQUEST (PROGRAM DATA OF NEW FIRMWARE, CHALLENGE DATA)

S1.2: FIRMWARE UPDATE REQUEST (PROGRAM DATA OF NEW FIRMWARE, CHALLENGE DATA)

S1.3: STORE FIRMWARE

S1.4: GENERATE DIGITAL SIGNATURE OF CHALLENGE

S1.5: RETAIN RESPONSE DATA

S1.6: COMMAND

S1.7: RESPONSE DATA REQUEST

S1.8: ACQUIRE RESPONSE DATA

S1.9: COMMAND (DIGITAL SIGNATURE)

S1.10: UPDATE COMPLETION NOTIFICATION (DIGITAL SIGNATURE)

FIG. 4

200: DELIVERY SERVER

201: TIMER

300: IP NETWORK

100: TERMINAL DEVICE

1: MEMORY DEVICE

FIG. 5

S2.1: ISSUE FIRMWARE UPDATE REQUEST

S2.2: ACTIVATE TIMER

S2.4: IS THERE RESPONSE ?

S2.5: IS SUCCESSFUL RESPONSE AUTHENTICATION ?

UPDATE FAILs

UPDATE IS SUCCESSFUL

FIG. 6

1: MEMORY DEVICE

10: DATA TRANSMISSION UNIT

30: ENCRYPTION PROCESSING UNIT

31: ENCRYPTION CALCULATION UNIT

32: RANDOM NUMBER GENERATION UNIT

70: SECRET KEY STORAGE AREA

80: PUBLIC KEY STORAGE AREA

20: DATA RECEIVING UNIT

50: RESPONSE DATA STORAGE AREA

60: DIGITAL SIGNATURE GENERATION UNIT

40: FIRMWARE STORAGE AREA

35: AUTHENTICATION UNIT

FIG. 7

200: DELIVERY SERVER

203: DIGITAL SIGNATURE GENERATING UNIT

202: SECRET KEY STORAGE AREA

201: TIMER

300: IP NETWORK

100: TERMINAL DEVICE

1: MEMORY DEVICE

FIG. 8

200: DELIVERY SERVER

100: TERMINAL DEVICE

1: MEMORY DEVICE

S3.1: FIRMWARE UPDATE REQUEST (PROGRAM DATA OF NEW FIRMWARE, FIRST CHALLENGE DATA)

S3.2: FIRMWARE UPDATE REQUEST (PROGRAM DATA OF NEW FIRMWARE, FIRST CHALLENGE DATA)

S3.3: STORE FIRMWARE

S3.4: GENERATE FIRST DIGITAL SIGNATURE OF FIRST CHALLENGE DATA

S3.5: RETAIN FIRST RESPONSE DATA

S3.6: COMMAND

S3.7: FIRST RESPONSE DATA REQUEST

S3.8: ACQUIRE FIRST RESPONSE DATA

S3.9: GENERATE SECOND CHALLENGE DATA

S3.10: COMMAND (FIRST DIGITAL SIGNATURE, SECOND CHALLENGE DATA)

S3.11: SECOND RESPONSE DATA REQUEST (FIRST DIGITAL SIGNATURE, SECOND CHALLENGE DATA)

S3.12: GENERATE SECOND DIGITAL SIGNATURE OF SECOND CHALLENGE DATA

S1.13: COMMAND (SECOND DIGITAL SIGNATURE)

S3.14: COMMAND (SECOND DIGITAL SIGNATURE)

FIG. 9

1: MEMORY DEVICE

10: DATA TRANSMISSION UNIT

30: ENCRYPTION PROCESSING UNIT

31: ENCRYPTION CALCULATION UNIT

32: RANDOM NUMBER GENERATION UNIT

70: SECRET KEY STORAGE AREA

20: DATA RECEIVING UNIT

50: RESPONSE DATA STORAGE AREA

60: DIGITAL SIGNATURE GENERATION UNIT

90: PATCH DATA STORAGE AREA

FIG. 10

200: DELIVERY SERVER

100: TERMINAL DEVICE

1: MEMORY DEVICE

S4.1: PATCH APPLICATION REQUEST (PATCH DATA, CHALLENGE DATA)

S4.2: PATCH APPLICATION REQUEST (PATCH DATA, CHALLENGE DATA)

S4.3: STORE PATCH DATA

S4.4: GENERATE DIGITAL SIGNATURE OF CHALLENGE

S4.5: RETAIN RESPONSE DATA

S4.6: COMMAND

S4.7: RESPONSE DATA REQUEST

S4.8: ACQUIRE RESPONSE DATA

S4.9: COMMAND (DIGITAL SIGNATURE)

S4.10: PATCH APPLICATION COMPLETION NOTIFICATION (DIGITAL SIGNATURE)