

【DESCRIPTION】**【Title of Invention】**

SMART CARD DEVICE, APPARATUS FOR GENERATING VIRTUAL
SECURITY CODE THROUGH DETERMINATION OF WHETHER DATA ARE
5 IDENTICAL TO EACH OTHER, AND METHOD THEREOF

【Technical Field】

[1] The present disclosure relates to a smart card device, an apparatus for generating a
virtual security code through determination on whether data are identical to each other, and a
method thereof.

10 **【Background Art】**

[2] Code-type data is used in many areas. Code-type data includes not only the card
number and account number used for payment, but also the IPIN number and social security
number for user identification.

[3] However, the code data is sometimes leaked during the use thereof. In the case of the
15 card number, the actual card number is shown on the surface of the card, so it is visually
leaked to others, and when payment is made using a magnetic technology, the card number is
leaked to a POS device.

[4] There were many attempts to use a virtual code to prevent the actual code from being
leaked, but data, which is used to identify the user to search for the actual code corresponding
20 to the virtual code, was necessary.

[5] However, in the case of one-time password (OTP), a separate OTP generating device
is required, which is inconvenient, and particularly, a user terminal is weak in terms of
security due to the leakage of seed data used to generate OTP.

[6] Therefore, there is a need for a method of improving security by not requiring a
25 separate OTP generating device and preventing the leakage of seed data while generating an

OTP code like a virtual security code necessary for user authentication based on card data of a card held by a lot of users. However, appropriate solutions to solve these problems have not yet been suggested.

【Disclosure】

5 【Technical Problem】

[7] An object of the present disclosure is to provide a smart card device, an apparatus for generating a virtual security code through determination on whether data are identical to each other, and a method thereof.

[8] Technical objects to be achieved by the present disclosure are not limited to the
10 aforementioned technical objects, and other technical objects not described above may be evidently understood by a person having ordinary skill in the art to which the present disclosure pertains from the following description.

【Technical Solution】

[9] A method performed by a virtual security code generation device according to an
15 aspect of the present disclosure to solve the above problems includes receiving seed data and a chip eigen value which are needed for generating a virtual security code from a card when an IC chip and an NFC chip are tagged with the card, determining whether the received chip eigen value is identical to a prestored chip eigen value, and generating a virtual security code based on the seed data and time data corresponding to a time point of receiving the seed data,
20 if the received chip eigen value is identical to the prestored chip eigen value.

[10] In the present disclosure, the method may further include transmitting a command and a user key value to the card when tagged with the card, and receiving the seed data from the card according to whether the user key value is normal.

[11] In the present disclosure, the card may determine whether the user key value is
25 identical to the prestored user key value, and the seed data may be transmitted to the virtual

security code generation device if the user key value is identical to the prestored user key value.

[12] In the present disclosure, the user key value is a unique value allocated to the user to map the user to the card issued to the user, and the user key value may be combined with the command and transmitted.

[13] In the present disclosure, a card number, seed data, the user key value and the chip eigen value may be allocated to the user, to which the card is to be issued, when issuing the card.

[14] In the present disclosure, when the user registers the card in an application in the virtual security code generation device, the chip eigen value may be received from the card through the card tagging and may be stored in the application, and may be transmitted to a server through the virtual security code generation device and may be mapped to user identification information and may be stored in the server.

[15] In the present disclosure, the method further includes requesting user authentication by transmitting the virtual security code to a server, wherein the server may extract the user identification information by searching for a storage location of user identification information based on the virtual security code, and perform user authentication based on the extracted user identification information.

[16] In the present disclosure, the virtual security code includes a plurality of detailed codes, and the plurality of detailed codes may include a first code which sets a starting point of a search of a storage location of the user identification information and a second code which sets a search route of from the starting point to the storage location of the user identification information, according to the predetermined search scheme.

[17] A smart card device according to another aspect of the present disclosure to solve the above problems includes an NFC module which performs NFC-based communication when

tagged with a virtual security code generation device, and an IC module which stores data for generating a virtual security code through an applet, wherein the IC module transmits a chip eigen value and seed data necessary for generation of the virtual security code, to the virtual security code generation device, through the NFC module, when tagged with the virtual security code generation device, and wherein, if the transmitted chip eigen value is identical to the chip eigen value prestored in the virtual security code generation device, the virtual security code is generated based on the seed data and time data corresponding to a time point of receiving the seed data.

[18] In the present disclosure, the IC module may receive a command and a user key value from the virtual security code generation device through the NFC module, when tagged with the virtual security code generation device, determine whether the received user key value is identical to the prestored user key value, and transmit the seed data to the virtual security code generation device if the received user key value is identical to the prestored user key value.

[19] In addition, another method, another system, and a computer-readable recording medium having, recorded thereon, a computer program for executing the method for implementing the present disclosure may be further provided.

【Advantageous Effects】

[20] According to the present disclosure, a user can create a virtual security code for user authentication using card data obtained based on a NFC scheme without a separate OTP device.

[21] In addition, since a smart card device determines whether a user key value is normal, and provides a virtual security code generation device with seed data for the creation of a virtual security code only when the user key value is normal, it can prevent exposure of seed data.

[22] In addition, since the virtual security code generation device determines whether a chip eigen value is normal and generates a virtual security code only when the chip eigen value is normal, abnormal access by card replication can be prevented.

[23] The effects of the present disclosure are not limited to the effect mentioned above, and other effects that are not mentioned can be clearly understood by one of ordinary skill in the art from the following description.

【Description of Drawings】

[24] FIG. 1 is a block diagram of a system which generates a virtual security code by determining whether data are identical to each other according to the present disclosure.

10 [25] FIG. 2 is a block diagram schematically illustrating a smart card device according to the present disclosure.

[26] FIG. 3 is a block diagram schematically illustrating a virtual security code generation device according to the present disclosure.

15 [27] FIG. 4 is a flowchart of a system which generates a virtual security code by determining whether data are identical to each other according to the present disclosure.

[28] FIG. 5 is a diagram illustrating generation of a virtual security code by confirming a chip eigen value according to the present disclosure.

[29] FIG. 6 is a diagram illustrating generation of a virtual security code by confirming a user key value according to the present disclosure.

20 [30] FIG. 7 is a diagram illustrating generation of a virtual security code by confirming a chip eigen value and a user key value according to the present disclosure.

【Mode for Disclosure】

[31] The advantages and features of the present disclosure, and the method of achieving them will become clear by referring to the embodiments described in detail with the accompanying drawings. However, the present disclosure is not limited to the embodiments

25

disclosed below and can be implemented in different forms, and only these embodiments are provided to complete the present disclosure and to fully inform one of ordinary skill in the art of the scope of the present disclosure, and the present disclosure is only defined by the claims.

[32] The terms used herein are for explaining embodiments and are not to limit the present disclosure. In the present disclosure, a singular expression also includes a plural expression unless specifically mentioned otherwise. "Comprises" and/or "comprising" used in the present specification do not exclude the presence or addition of one or more other components in addition to the components mentioned. The same reference numeral refers to the same component, and "and/or" includes each and or more combinations of the mentioned components throughout the specification. Although "first" and "second" are used to describe various components, these components are not limited by these terms. These terms are used only to distinguish them from other components. Therefore, the first component mentioned below may also be a second component within the technical idea of the present disclosure.

[33] All the terms used herein (including technical and scientific terms) can be used in common by one of ordinary skill in the related art unless there are other definitions. In addition, the terms that are commonly used in the dictionary are not ideally or excessively interpreted unless they are clearly defined.

[34] Hereinafter, preferred embodiments of the present disclosure will be described in detail with reference to the accompanying drawings.

[35] Prior to the detailed description, the meanings of the terms used in this specification are briefly described. However, the description of the terms is intended to help an understanding of the present disclosure, so it should be noted that if it is not explicitly stated as a matter that limits the present disclosure, the description is not used to limit the technical idea of the present disclosure.

[36] In this specification, "letter" is a component that constitutes a code and includes all

or part of uppercase alphabets, lowercase alphabets, numbers, and special characters.

[37] In this specification, "code" means a string of letters.

[38] In this specification, "virtual security code" is a random code (e.g., a one-time password (OTP), which is temporarily generated for user authentication and is changed per unit time, and may include a specific digit code consisting of letters. The virtual security code can be used to search for the identification information of the user stored in the server according to an embodiment of the present disclosure.

[39] In addition, the "virtual security code" may include a virtual code for authentication (e.g., one-time authentication code (OTAC)) which is temporarily generated for the user authentication, and a random code (e.g., a one-time password (OTP)) which is used for second authentication after first authentication of the user is performed through the virtual code for authentication.

[40] In this specification, "smart card device" refers to a card that provides data for creating a virtual security code. In addition, the smart card may be an arbitrary card for financial transactions, such as a credit card, a check card, and a cash card, and there is no limitation to the type and purpose of the card.

[41] In the present specification, the "virtual security code generation device" is a terminal used by a user, and is a random electronic device with an application processor (AP) that can run an application. The user terminal includes a non-portable desktop computer or a portable mobile device (e.g., a smartphone, a tablet PC, a personal digital assistant (PDA), an enterprise digital assistant (EDA), a portable multimedia player (PMP), a personal navigation device (PND), and a wearable device), but is not limited thereto.

[42] In this specification, the "virtual security code generation function" refers to a function that generates a virtual security code. For example, the function includes one-time password (OTP), but is not limited thereto.

[43] In this specification, the "detailed code generation function" refers to a function that generates each detailed code that constitutes a virtual security code.

[44] In the present specification, the "detailed code combination function" refers to a function that generates a virtual security code by combining a plurality of detailed codes.

5 [45] In this specification, "user identification (UID)" refers to a unique code-type value that is given for each user to identify the user.

[46] In the present disclosure, "unit count" is a unit which is set at specific time intervals and is changed when the time interval passes. For example, "1 count" may be set as a specific time interval (e.g., 1.5 seconds).

10 [47] In this specification, "storage location" refers to a point on a track, which corresponds to a time point when card registration has been requested by a user.

[48] Hereinafter, preferred embodiments of the present disclosure will be described in detail with reference to the accompanying drawings.

[49] FIG. 1 is a block diagram of a system which generates a virtual security code by
15 determining whether data are identical to each other according to the present disclosure.

[50] FIG. 2 is a block diagram schematically illustrating a smart card device according to the present disclosure.

[51] FIG. 3 is a block diagram schematically illustrating a virtual security code generation device according to the present disclosure.

20 [52] FIG. 4 is a flowchart of a system which generates a virtual security code by determining whether data are identical to each other according to the present disclosure.

[53] FIG. 5 is a diagram illustrating generation of a virtual security code by confirming a chip eigen value according to the present disclosure.

[54] FIG. 6 is a diagram illustrating generation of a virtual security code by confirming a
25 user key value according to the present disclosure.

[55] FIG. 7 is a diagram illustrating generation of a virtual security code by confirming a chip eigen value and a user key value according to the present disclosure.

[56] Referring to FIG. 1, a system for generating a virtual security code (hereinafter, referred to as "system") through determination on whether data are matched with each other includes a smart card device 10, a virtual security code generation device 20, and a server 30. Here, the system may include fewer components or more components than the components shown in FIG. 1.

[57] The smart card device 10 means a real card used by the user. Depending on the embodiment, only a portion of the information that can identify the card or user may be displayed on the surface of the smart card device 10, or no information may be displayed.

[58] The virtual security code generation device 20 generates a virtual security code for user authentication based on the card data received from the smart card device 10.

[59] More specifically, a program or application in the virtual security code generation device 20 generates a virtual security code based on the seed data obtained from the smart card device 10. To this end, the program or application may include an OTP function.

[60] The seed data of the smart card device 10 may include the user identification information [UID (User ID)] of the smart card device 10. Here, the user identification information may be created based on the information entered from the user or the log-in information of the user. Specifically, when a user logs in to a program or an application and applies for issuance of a card, the server 30 maps user identification information based on the user's login information to data related to the card to be issued to the user. This mapped information can be stored in the server 30.

[61] However, the user identification information of the present disclosure is not limited thereto and may be set or used as user information as specific unique information, which is set as a default at the time of producing a smart card device 10, and may be mapped to a specific

user, unlike what is not set by a user, such as a serial number of the smart card device 10. In addition, the user identification information may include personal information, such as social security number, bank account number, and credit card number, as well as UID.

[62] As described above, the virtual security code generation device 20 generates a virtual security code based on seed data obtained from the smart card device 10. At this time, the virtual security code may be created by a one-time password (OTP) function. In this case, the virtual security code is generated based on seed data, and time data at a time point when seed data and virtual security code were requested, or a time point when seed data was obtained.

[63] Specifically, the virtual security code is generated by a virtual security code generation function included in the virtual security code generation device 20, and particularly, the virtual security code may include one or more detailed codes, which will be described in detail later.

[64] On the other hand, the server 30 performs user authentication based on the virtual security code received from the virtual security code generation device 20. At this time, the server 30 may be a financial company server that communicates with the virtual security code generation device 20, but is not limited thereto. Further, referring to FIG. 1, it is illustrated that the server 300 is composed of one server, but it may also be formed as a system where a plurality of servers are connected to each other.

[65] On the other hand, according to an embodiment of the present disclosure, the server 30 may further perform a process of verifying whether the received virtual security code has been normally generated or used twice

[66] As shown in FIG. 1, the smart card device 10, the virtual security code generation device 20, and the server 30 may send and receive various data, signals or information through the communication network.

[67] Here, various forms of communication networks can be used. For example, wireless

communication schemes such as Wireless LAN (WLAN), Wi-Fi, Wibro, Wimax, and high speed downlink packet access (HSDPA), or wired communication schemes such as Ethernet, xDSL (ADSL, VDSL), hybrid fiber coax (HFC), fiber to the curb (FTTC), and fiber to the home (FTTH) may be used.

5 **[68]** Here, the communication network is not limited to the communication method presented above, and may include all forms of communication methods that is known or will be developed in the future, in addition to the above-described communication methods.

10 **[69]** Referring to FIG. 2, the smart card device 10 may include an NFC module 12 and an IC module 14. Here, the smart card device 10 may include fewer components or more components than the components shown in FIG. 2.

[70] A narrow frequency communication (NFC) module 12 is a communication module and may perform NFC-based communication when tagged with the virtual security code generation device 20.

15 **[71]** The IC module (i.e., IC chip) may store data for generating a virtual security code through an applet.

[72] The IC module 14 is mounted on a PCB plate to contact the terminal of an IC card reader to perform the data exchange. The IC module 14 may include parts including an integrated circuit (IC) and a system on chip (SoC). For example, the IC chip may be an ISO 14443 NXP Mifare Classic type according to the present disclosure, but is not limited thereto.

20 **[73]** In addition, although not shown in the drawing, the smart card device 10 may include a memory (not shown) that stores the card data. Here, the card data may include all the data necessary for the creation of a virtual security code. More specifically, the card data may include user identification information of the user, who applied for issuance of the smart card, and card identification information of the card issued to the user.

25 **[74]** The applet stores card data in the smart card device 10. In an embodiment of the

present disclosure, the applet of the smart card device 10 may store the card data in the storage area of the memory based on the NFC Data Exchange Format (NDEF). That is, the card data is stored in the smart card device 10 in a standardized NDEF format so that the smart card device 10 and the virtual security code generation device 20 can mutually exchange information through NFC.

[75] The IC module 14 may transmit data necessary for the creation of the virtual security code to the virtual security code generation device 20 through the NFC module 12 when tagging with the virtual security code generation device 20. At this time, the data transmitted may be seed data and chip eigen value, but are not limited thereto. Here, the chip eigen value may be an eigen value of the IC chip, or an eigen value of the NFC chip.

[76] If the transmitted chip eigen value is identical to the chip eigen value prestored in the virtual security code generation device 20, the virtual security code may be generated based on the seed data and time data corresponding to the time point of receiving the seed data (or time point of requesting generation of a virtual security code). Details thereof will be described later.

[77] In addition, when tagging with the virtual security code generation device 20, the IC module 14 receives a command and a user key value from the virtual security code generation device 20 through the NFC module 12 and determines whether the received user key value is identical to the prestored user key value. If the received user key value is identical to the prestored user key value, the IC module 14 may transmit the seed data to the virtual security code generation device 20. Details thereof will be described later.

[78] Referring to FIG. 3, the virtual security code generation device 20 may include a communication unit 22, a memory 24 and a processor 26. Here, the virtual security code generation device 20 may include fewer components or more components than the components shown in FIG. 3.

[79] If the smart card device 10 is tagged with the virtual security code generation device 20, the communication unit 22 may transmit a user key value and a command to request a result of the chip eigen value to the smart card device 10, through the communication network, and may receive seed data and chip eigen value from the smart card device 10. In addition, the two devices can transmit and receive various data from each other during tagging.

[80] The memory 24 may store data that supports various functions of the virtual security code generation device 20. The memory 24 may store a plurality of application programs operated in the virtual security code generation device 20, at least one process, data, and commands for operation of the virtual security code generation device 20. At least some of these applications may exist for the basic function of the virtual security code generation device 20.

[81] In addition to the operation related to the application, the processor 26 may generally control the overall operation of the virtual security code generation device 20. The processor 26 may provide appropriate information to the smart card device 10 or server 30 or process such information by processing signals, data, information, etc. input or output through the components shown above, or by driving the application stored in the memory 24.

[82] The processor 26 may control at least some of the components discussed with reference to FIG. 3 in order to drive an application program stored in memory 24. Further, the processor 26 may operate two or more of the components included in the virtual security code generation device 20 in combination with each other in order to drive the application program.

[83] Referring to FIG. 3, the processor 26 may include a code generation unit 262 and a verification request unit 264. Here, the processor 26 may include fewer components or more components than the components shown in FIG. 3.

[84] The code generation unit 262 may generate a virtual security code using the seed data and time data received from the smart card device 10.

[85] The verification request unit 264 may transmit the virtual security code to the server 30 through the communication unit 22 to request the server 30 to verify the virtual security code and perform a user authentication.

[86] Although not shown in FIG. 3, the processor 26 may further include components that perform various computation operations and determination operations, in addition to the code generation unit 262 and the verification request unit 264.

[87] Hereinafter, a method of generating a virtual security code by the virtual security code generation device 20 is explained with reference to FIGS. 4 to 7.

[88] Referring to FIG. 4, the virtual security code generation device 20 may receive the seed data and chip eigen value required for the creation of the virtual security code from the card when the IC chip and NFC chip tags a card embedded therein (S110). Here, the card may mean the smart card device 10 described above.

[89] The virtual security code generation device 20 may determine whether the received chip eigen value matches the prestored chip eigen value (S120).

[90] If the received chip eigen value matches the prestored chip eigen value, the virtual security code generation device 20 may generate a virtual security code, based on the seed data and time data corresponding to the time point of receiving the seed data (S130).

[91] Herein, the chip eigen value may be an eigen value of the IC chip or an eigen value of the NFC chip, but hereinafter, it is assumed that the chip eigen value is the eigen value of the IC chip.

[92] The virtual security code generation device 20 determines whether the received chip eigen value is identical to the chip eigen value prestored in the device and generates a virtual security code only when the two values are identical to each other, in order to prevent an abnormal access of requesting payment by copying chip data of the card. That is, although hackers can duplicate chip data in the card, they do not know the eigen value of the chip itself

when manufacturing the chip. Hence, the virtual security code generation device 20 generates a virtual security code for payment after determining whether the received chip eigen value is a normal value. In this regard, details will be explained with reference to FIG. 5.

[93] Referring to FIG. 5, when the smart card device 10 is tagged to the virtual security code generation device 20, the virtual security code generation device 20 transmits a command to the smart card device 10 (S51). Here, the command may be a command requesting a return of a chip eigen value. The smart card device 10 transmits the chip eigen value to the virtual security code generation device 20 in response to the command (S52). The virtual security code generation device 20 determines whether the received chip eigen value matches the prestored chip eigen value (S53). If the received chip eigen value matches the prestored chip eigen value, the virtual security code generation device 20 generates a virtual security code using seed data received from the smart card device 10, and time data obtained at the time point of receiving the seed data (or time point of requesting generation of the virtual security code) (S54).

[94] On the other hand, although not shown in FIG. 4, the virtual security code generation method performed by the virtual security code generation device of the present disclosure may further include a step of transmitting a command and a user key value to the card at the time of tagging the card, and a step of receiving the seed data from the card, depending on whether the user key value is normal. Here, the card may mean the smart card device 10 described above.

[95] That is, the card determines whether the user key value matches the prestored user key value, and when the user key value matches the prestored user key value stored, the card may transmit the seed data to the virtual security code generation device 20.

[96] Here, the user key value is a unique value allocated to the user to map the user to the card issued to the user. That is, when a user joins the application and applies for a card

issuance, the server 30 may map the card to the user by setting the user key value for the card to be issued to the user.

[97] The user key value may be transmitted in a form combined with the command when transmitted to the card. In more detail, the user key value may be transmitted to the smart card device 10 in the form combined behind an application protocol data unit (APDU) command. However, the combined form is not limited thereto.

[98] The smart card device 10 determines whether the received user key value is identical to the user key value prestored in the device, and transmits seed data only when the two values are identical to each other, in order to prevent the exposure of the seed data to a person who is not the user. In this regard, details will be explained with reference to FIG. 6.

[99] Referring to FIG. 6, the virtual security code generation device 20 transmits a user key value in a form combined with a command, to the smart card device 10 (S61). The smart card device 10 determines whether the received user key value matches the prestored user key value (S62). As a result of the determination, if two user key values are identical to each other, the smart card device 10 transmits the seed data to the virtual security code generation device 20 (S63). The virtual security code generation device 20 generates a virtual security code using the received seed data and the time data obtained at the time point when the seed data was received (S64).

[100] In summary, in the present disclosure, if a smart card device 10 is tagged to the virtual security code generation device 20, a process of determining whether data are identical to each other is performed in each of the smart card device 10 and the virtual security code generation device 20, and the virtual security code is generated only when both determination results are normal. As such, the security may be improved in generating a virtual security code.

[101] Referring to FIG. 7, the virtual security code generation device 20 transmits a chip

eigen value return request command to the smart card device 10, and in this case, a user key value is combined with the command, which are then transmitted together (S71). The smart card device 10 determines whether the received user key value is normal (S72). If the received user key value is identical to the prestored user key value, the chip eigen value together with the seed data is transmitted to the virtual security code generation device 20, in response to the command (S73). The virtual security code generation device 20 determines whether the received chip eigen value is normal (S74). If the received chip eigen value is identical to the prestored chip eigen value, a virtual security code is generated using the received seed data, and time data of the point of time of receiving the seed data (time point of requesting generation of a virtual security code) (S75).

[102] In this case, if the received user key value is not identical to the prestored user key value, the smart card device 10 may not transmit the seed data to the virtual security code generation device 20. According to an embodiment, the smart card device 10 may transmit a chip eigen value to the virtual security code generation device 20 in response to the command regardless of whether the seed data has been transmitted, but a virtual security code cannot be generated because the seed data has not been transmitted.

[103] In addition, it was illustrated above that the user key value is combined with the chip eigen value return request command and is then transmitted together, but the chip eigen value return request command may be different from a command with which the user key value is combined, depending on the embodiment. That is, when a card is tagged, the virtual security code generation device 20 may transmit each of the chip eigen value return request command and the command, with which the user key value has been combined.

[104] Hereinafter, a specific method of generating a virtual security code according to an embodiment of the present disclosure, will be described.

[105] The code generation unit 262 plays a role of generating one or more detailed codes.

The detailed code means some codes that constitute a virtual security code. The virtual security code may be configured only by detailed codes, or may be formed in the form of the final virtual security code (OTAC) by combining one or more detailed codes to a first virtual security code generated by the OTP function.

5 **[106]** The virtual security code generation device 20 includes a virtual security code generation function which generates a virtual security code, and the virtual security code generation function includes a detailed code generation function which generates one or more detailed codes, and a detailed code combination function (that is, a rule of combining one or more detailed codes) which generates a virtual security code by combining with the detailed
10 codes.

[107] That is, when a virtual security code includes a plurality of detailed codes, the virtual security code generation function generates a plurality of detailed codes using a plurality of detailed code generation functions, and generates a virtual security code by combining the plurality of detailed codes as a predetermined combination through the detailed code
15 combination function.

[108] According to an embodiment, the code generation unit 262 may generate the virtual security code by the detailed code generation function based on the seed data obtained as the smart card device 10 is tagged.

[109] The plurality of detailed codes have a correlation which is used for the server 30 to
20 search for the storage space of the user identification information. That is, the server 30 includes a search algorithm (storage space search algorithm), and the search algorithm extracts a plurality of detailed codes included in the virtual security code received from the virtual security code generation device 20, and searches for the storage space of the user identification information (UID), based on the correlation between the plurality of detailed
25 codes. As an embodiment about the correlation between the plurality of detailed codes, a

search algorithm included in the server 30 may search for the storage location of the user identification information by performing computations based on the correlation between the plurality of detailed codes from the pass points corresponding to one or more detailed codes among the plurality of detailed codes. At this time, there may be one or more pass points, and
5 there is no limitation to the number or order.

[110] In addition, as an embodiment of a plurality of detailed codes, the plurality of detailed codes may include a first code and a second code, and the code generation unit 262 includes a first function and a second function as the detailed code generation function and generates a first code and a second code. The first code and the second code have a
10 correlation for searching for the storage space of the user identification information in the server 30, but the virtual security code generation device 20 only includes a first function which generates a first code, and a second function which generates a second code, as the detailed code generation function, but may not include data about the correlation between the first code and the second code.

[111] As a specific example of the correlation between the first code and the second code, the first and second code can each play a role for searching for the storage space of the user identification information (UID). That is, the first code may include information about the pass point, and the second code may include information necessary for the operation for reaching the storage space of the user identification information from the pass point.

[112] On the other hand, as an embodiment of the present disclosure, the first code may be generated based on the first count, and the second code may be generated based on the second count. At this time, the first count is the number of unit counts that have elapsed from the initial time point, when the virtual security code generation function was operated, to a time point, when a virtual security code was generated, and the second count may include the
20 number of unit counts which have elapsed from the time point when the user identification
25

information (UID) of the user was registered in the server, or the time point when the user's smart card device 10 was issued and was then registered in the server 30 through the virtual security code generation device 20.

[113] That is, the first function that generates the first code is a function that provides a specific code value corresponding to the first count, and the second function that generates the second code is a function that provides a specific code value corresponding to the second count.

[114] Through this, it is possible to set the same virtual security code not to be redundantly generated, regardless of the generation time of the virtual security code and the user. For example, the first code is as any one code value [for example, a code value corresponding to a time point (or count) when generation of a virtual security code was requested] among codes matched for each count from the initial time point when the first function was operated in the server 300, and the virtual security code generation device 20 generates a first code having a different code value for each period when the virtual security code is generated in the same user.

[115] In addition, even in the case of the same time point, each virtual security code generation device 20 always has a different second count value, and thus the virtual security code generation device 20 always generates a different second code at the same time point. That is, the first code becomes a different code value for each count, and the second code has a different code value for each app card application installed in the virtual security code generation device 20 of each user at the same point of time. As such, the virtual security code (OTAC), which is the combination of the first code and the second code, is output as a code value which is always different or is not redundant, regardless of the user or virtual security code generation request time.

[116] In addition, in another embodiment, the virtual security code generation function

may generate the N-digit first code or the N-digit second code using M letters, and in this case, the virtual security code generation function includes first function and a second function which respectively provide the first code or the second code, in which different $M \times N$ codes are changed sequentially per unit count. That is, the first function or the second function is a function which generates $M \times N$ codes in a manner that is not redundant as the count increases, and a specific one among $M \times N$ codes is generated as the first code or the second code at a count corresponding a specific time point. Through this, the virtual security code generation device 20 does not redundantly generate the same first code or second code within $M \times N$ counts (that is, time period corresponding to $M \times N$ counts), and generates a new detailed code (that is, the first code or the second code) per unit count, to thereby generate a new virtual security code (OTAC) per unit count.

[117] Specifically, when the virtual security code generation function uses $M \times N$ codes as the first code or the second code as the N-digit first code or second code is generated using M letters, the first code or the second code is matched for each count from the initial time point when the detailed code generation function is operated.

[118] For example, when the unit count is set to the second count, different $M \times N$ codes are matched every second from the time point when the detailed code generation function is operated for the first time. Further, if a period for using a specific detailed code generation function, or a use period of a program or an application for generation of a virtual security code in the virtual security code generation device 20, is set to be shorter than a time length corresponding to $M \times N$ counts (e.g., if one count is 1 second, $M \times N$ seconds), the first code or the second code is not redundantly generated as the same code during the use period. That is, when the count increases over time, if the user generates a virtual security code at a specific time point, the virtual security code generation device 20 may generate a code value, which is matched to a count corresponding to a specific time point, as the first code or the

second code.

[119] Further, various schemes may be applied as a scheme of generating one virtual security code (OTAC) by combining a plurality of detailed codes. As an example of the detailed code combination function, a virtual security code may be generated in a manner that
5 a M-digit first code and an N-digit second code are alternately arranged.

[120] In addition, as another example, the detailed code combination function may generate a virtual security code in a manner that combines the second code behind the first code. As the number of detailed codes included in the virtual security code increases, the virtual security code can be generated in various ways in a manner that is not redundant. The
10 code generation unit 262 plays a role of combining one or more detailed codes to generate a virtual security code.

[121] On the other hand, a virtual security code generation method performed by the virtual security code generation device of the present disclosure may further include a step of transmitting the virtual security code to the server to request user authentication.

[122] The server 30 may extract the user identification information by searching for the storage location of the user identification information based on the virtual security code, and perform a user authentication based on the extracted user identification information.
15

[123] Here, the virtual security code includes a plurality of detailed codes, and the plurality of detailed codes may include a first code which sets the starting point of the storage location
20 search of the user identification information, and a second code which sets the search route of from the starting point to the storage location of the user identification information, according to the predetermined search scheme.

[124] Hereinafter, a method of verifying a virtual security code in the server 30 and authenticating a user based on the verified virtual security code will be described.

[125] As an embodiment of the present disclosure, when the server 30 receives the virtual
25

security code from the virtual security code generation device 20, the received virtual security code may be verified by comparing the received time data with the time data of the virtual security code.

[126] Specifically, the server 30 verifies whether the virtual security code delivered through the virtual security code generation device 20 has normally been generated. That is, the server 30 determines whether the virtual security code is normal by receiving the virtual security code and then determining whether the received virtual security code has normally been generated at the time point of requesting financial transactions based on the information stored in the server 30 (that is, virtual security code generation function and seed data). For example, the server 30 and (for example, a financial company server) determines whether there is a value identical to the virtual security code among OTP numbers which were obtained by inputting a count within a specific range from the count at which a virtual security code was received using the virtual security code generation function (that is, OTP function). The server 30 applies the inverse function of the virtual security code generation function to the virtual security code to find a count corresponding to the time point when the virtual security code was created. Since the count at which the server 30 receives the virtual security code may not be identical to the count at which the OTP number corresponding to the virtual security code is generated due to the difference between the time point when the virtual security code is generated in the virtual security code generation device 20 and the time point when the server 30 receives the virtual security code, due to the transmission time of the virtual security code or delay, the server 30 allows a tolerance from the count at which the virtual security code is received.

[127] Further, according to an embodiment of the present disclosure, the server 30 may extract the user identification information by searching for the storage location of the user identification information based on the virtual security code, and perform a user

authentication based on the extracted user identification information.

[128] Here, as described above, the virtual security code includes a plurality of detailed codes, and the plurality of detailed codes may include a first code which sets the starting point of the storage location search of the user identification information, and a second code which sets the search route of from the starting point to the storage location of the user identification information, according to the predetermined search scheme.

[129] In addition, as a specific example of the first code and the second code, the code value (first code value) corresponding to the first code may be a value which is obtained by adding the first virtual security code value to the OTP code at a count corresponding to the current time point, based on the time point of operating the virtual security code generation function. The first code value plays a role as a pass point during the actual code search process. The code value (second code value) corresponding to the second code may be a value which is obtained by subtracting the storage location value of the user identification information (e.g., UID) from the first code. The second code value is a count of from the pass point (first code value) to the storage location value of the user identification information.

[130] That is, an example of a first code and a second code which are generated by the virtual security code generation device 20 is as follows.

[131] First code = count at current time point + OTP code (first virtual security code)

[132] Second code = first code - storage location value of actual code

[133] As described above, the final virtual security code may be composed of a first code, a second code, and a first virtual security code generated by an OTP function. At this time, the first virtual security code is a code generated by the OTP function and is a code that is generated differently every time. Thus, since the detailed code is generated differently depending on the time of the creation of the virtual security code, redundant generation of the detailed code may be prevented, and the security may be improved.

[134] As a specific example of the first code and second code, the code value corresponding to the first code (first code value) may be a value that is obtained by adding user identification information (UID) to the OTP code value, and the code value corresponding to the second code may be the OTP code value. In this case, the value of the user identification information (UID) is a code value which is given to a user or a virtual security code generation device 20 at a specific time point (e.g., a time point of manufacturing the card, a time point of registering the card, etc.) and is used to identify each user or virtual security code generation device 20.

[135] That is, another example of a first code, which is generated by the virtual security code generation device 20, is as follows. At this time, the virtual security code is created based on the first virtual security code and the first code.

[136] First code = OTP code (first virtual security code) + UID

[137] Hereinafter, a method of applying for a card issuance by a user and registering the issued card to a server will be described.

[138] When issuing a card at the user's request, the card number, the seed data, the user key value, and the chip eigen value for the user, to which the card is to be issued, may be allocated.

[139] More specifically, the user applies for a card issuance through an application within the virtual security code generation device 20. When the server 30 receives the card issuance application, the card number, seed data, and user key value of the card to be issued to the user are allocated and are mapped to the user identification information, and are then stored. That is, the card number, seed data and the user key value are set on the server.

[140] The server 30 delivers the card number, the seed data and the user key value while requesting a card issuance to a card issuing agency.

[141] The card issuing agency completes the card issuance by entering the card number, the seed data and the user key value on the card to be issued. At this time, the card issuing

agency delivers the chip eigen value to the server 30, and the server 30 additionally maps the delivered chip eigen value to the user identification information, and stores the mapping information. In this case, the chip eigen value is a value given to the chip when the chip contained in the card is produced, and since the chip eigen value is not set by the server 30, the server 30 should be provided the value from the card issuing agency.

[142] The user then requests registration of the card issued through the application in the virtual security code generation device 20. The server 30 transmits the user key value and the chip eigen value among data, which are mapped to the user identification information and stored, to the virtual security code generation device 20. The virtual security code generation device 20 may store the received user key value and chip eigen value and use the values later at the time of generating a virtual security code. However, the present disclosure is not limited thereto, and other data as well as the user key value and the chip eigen value may also be transmitted from the server 30 at the time of card registration, and stored in the virtual security code generation device 20.

[143] If the card registration is requested from the user as described above, the server 30 may start operating the virtual security code generation function for the user or the virtual security code generation device 20 at the time when the registration is requested, and may store user identification information at the count (point) corresponding to the time point when the registration is requested. Accordingly, the server 30 may perform user authentication by searching for user identification information from a virtual security code received from the virtual security code generation device 20 later.

[144] It was illustrated above that the chip eigen value is transmitted from the card issuing agency and stored in the server 30 before the card registration, but in some embodiments, the chip eigen value may be transmitted through a smart card device 10 at the time of card registration and stored in the server 30.

[145] When the user registers the card in an application in the virtual security code generation device 20, the chip eigen value may be received from the card through the card tagging and may be stored in the application, and may be transmitted to the server 30 through the virtual security code generation device 20 and may be mapped to user and may be stored
5 in the server 30.

[146] The method according to an embodiment of the present disclosure described above may be implemented as a program to be combined with a computer, which is hardware, and may be stored in a computer-readable recording medium.

[147] The program described above may include codes coded by a computer language such
10 as C, C++, JAVA, machine language, etc. readable through the device interface of the computer by the processor (CPI) of the computer, in order for the computer to read a program and execute the methods implemented by reading the program. Such codes may include functional codes related to functions that define the necessary functions to execute the methods, and include control codes related to execution procedures required to execute the
15 functions by the computer processor in a predetermined procedure. In addition, these codes may further include additional information which is necessary for the processor of the computer to execute the functions, or memory reference-related codes about at which location of the internal or external memory of the computer media should be referenced. In addition, if the processor of the computer needs to communicate with any other remote computer or
20 server to execute the functions, the codes may further include communication-related codes about information on how to communicate with any other remote computer or server using the communication module of the computer, and information on what information or media should be transmitted and received when communicated.

[148] The steps of the methods or algorithms described in connection with the
25 embodiments of the present disclosure may be implemented directly by hardware,

implemented as a software module executed by hardware, or by a combination thereof. A software module may reside in random access memory (RAM), read only memory (ROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory, a hard disk drive, a detachable disk drive, CD-ROM, or any
5 computer-readable recording medium.

[149] Although the embodiments of the present disclosure were described with reference to the accompanying drawings, it can be understood by one of ordinary skill in the art, to which the present disclosure belongs, that the present disclosure can be implemented in a different form without changing its technical ideas or essential features. Therefore, the embodiments
10 described above should be understood as exemplary in all aspects and should not be understood as limiting.

【CLAIMS】**【Claim 1】**

A method performed by a virtual security code generation device, the method comprising:

5 transmitting a command and a user key value to the card when tagged with the card;
 receiving seed data according to whether the user key value is normal and a chip eigen value which are needed for generating a virtual security code from a card when an IC chip and an NFC chip are tagged with the card;

 determining whether the received chip eigen value is identical to a prestored chip
 10 eigen value; and

 generating a virtual security code based on the seed data and time data corresponding to a time point of receiving the seed data, if the received chip eigen value is identical to the prestored chip eigen value.

15 **【Claim 2】**

The method of claim 1, wherein the card determines whether the user key value is identical to the prestored user key value, and

 wherein the seed data is transmitted to the virtual security code generation device if the user key value is identical to the prestored user key value.

20 **【Claim 3】**

The method of claim 1, wherein the user key value is a unique value allocated to the user to map the user to the card issued to the user, and

 wherein the user key value is combined with the command and is transmitted.

【Claim 4】

25 The method of claim 1, wherein a card number, seed data, the user key value, and the

chip eigen value are allocated to the user, to which the card is to be issued, when issuing the card.

【Claim 5】

5 The method of claim 4, wherein when the user registers the card in an application in the virtual security code generation device, the chip eigen value is received from the card through the card tagging and is stored in the application, and is transmitted to a server through the virtual security code generation device and is mapped to user identification information and is stored in the server.

【Claim 6】

10 The method of claim 1, further comprising: requesting user authentication by transmitting the virtual security code to a server,

wherein the server extracts the user identification information by searching for a storage location of user identification information based on the virtual security code, and performs user authentication based on the extracted user identification information.

15 **【Claim 7】**

The method of claim 6, wherein the virtual security code includes a plurality of detailed codes, and

wherein the plurality of detailed codes include:

20 a first code which sets a starting point of a search of a storage location of the user identification information; and

a second code which sets a search route of from the starting point to the storage location of the user identification information, according to the predetermined search scheme.

【Claim 8】

25 A program stored in a recording medium readable by a computer to execute a method according to any of claims 1 to 7 in combination with a computer.

【Claim 9】

A smart card device comprising:

an NFC module which performs NFC-based communication when tagged with a virtual security code generation device; and

5 an IC module which stores data for generating a virtual security code through an applet,

wherein the IC module

receives a command and a user key value from the virtual security code generation device through the NFC module, when tagged with the virtual security code generation device,

10 determines whether the received user key value is identical to a prestored user key value,

transmits a chip eigen value and seed data necessary for generation of the virtual security code, to the virtual security code generation device, through the NFC module, when tagged with the virtual security code generation device, if the received user key value is identical to the prestored user key value, and

15 wherein, if the transmitted chip eigen value is identical to a chip eigen value prestored in the virtual security code generation device, the virtual security code is generated based on the seed data and time data corresponding to a time point of receiving the seed data.

20