

【DESCRIPTION】

【Invention Title】

METHOD FOR REGISTERING USER IN HOLDERLESS CARD BY USING
AUTHENTICATION VIRTUAL CODE

5

【TECHNICAL FIELD】

[1] Embodiments of the inventive concept described herein relate to a method for registering a user in a holderless card by using an authentication virtual code.

10 **【BACKGROUND ART】**

[2] Code-type data is being used in a lot of fields. In addition to a card number or account number used to make a payment, the code-type data includes an IPIN number or a resident registration number for user identification.

[3] However, the code data may be leaked when the code data is used. In the case
15 of a card number, because an actual card number is recorded on a card surface as it is, the actual card number is visually exposed to other people. When a payment using a magnet is made, the card number is leaked to other people while being transmitted to a POS device.

[4] A virtual code has been used to prevent the actual code from being leaked.
20 However, there is a need for data for identifying a user to search for the actual code corresponding to the virtual code.

[5] However, a one-time password (OTP) is inconvenient because a separate OTP generating device is required. In particular, a user terminal has security vulnerabilities due to leakage of seed data used for OTP generation.

[6] Accordingly, an OTP code is generated in the same way as generating a virtual security code required for user authentication based on card data of a card possessed by many users. There is a need for a method of increasing security by not requiring a separate OTP generating device and preventing seed data from being leaked at the same time. However, an appropriate method for this has not yet been proposed.

【DETAILED DESCRIPTION OF THE INVENTION】

【TECHINICAL PROBLEM】

10 [7] Embodiments of the inventive concept provide a method for registering a user in a holderless card by using an authentication virtual code.

[8] Problems to be solved by the inventive concept are not limited to the problems mentioned above, and other problems not mentioned will be clearly understood by those skilled in the art from the following description.

15

【TECHNICAL SOLUTION】

[9] According to an embodiment, a method, which is performed by a holderless card having a physical form in a state where a user is not registered and which is used to register the user in the holderless card by using an authentication virtual code

20 includes receiving current time data from a terminal of the user through card tagging, generating a virtual code for authenticating the user based on the current time data and pre-stored seed data by using an applet included in the card, and requesting verification of the virtual code by transmitting the virtual code to a verification server through the user terminal. When the card is produced while the user is not registered,

and the verification is completed, the card is connected to the mobile card already owned by the user in the verification server such that the user is registered.

[10] Moreover, when the verification server is a server of a financial institution and the card is produced by a card manufacturer affiliated with the financial institution, the requesting of the verification may include requesting the verification by further transmitting at least one of a pre-stored card number of the card and a pre-stored eigenvalue of the card to the verification server through the user terminal. When the verification is completed, at least one of the seed data, the card number of the card, and the eigenvalue of the card may be matched with user information generated by the user terminal in the verification server so as to be stored.

[11] Furthermore, the card number of the card, the eigenvalue of the card, and the seed data may be delivered by the verification server to a server of the card manufacturer and may be embedded in an IC chip when the card is manufactured. The card number of the card may include an identification code of the financial institution, and the eigenvalue of the card may be a value sequentially assigned to each card manufactured by the card manufacturer.

[12] Besides, when the verification server is a service server providing a card issuance agency service, and the card is produced by a provider of the card issuance agency service, the user may be registered in a first method based on an application for physical card registration or a second method based on an interface for physical card registration.

[13] Also, the user terminal may be equipped with the application provided by the service server, and user registration in the first method may be made through the card tagging after a card number of the mobile card is entered through the application.

[14] In addition, the user registration in the first method may be made by the

service server by matching a card number of the card found based on the virtual code with the card number of the mobile card. The card number of the card may be transmitted from a payment server to the service server through a payment network when a payment is requested through the card for which the registration is
5 completed. The card number of the mobile card matched to the card number of the card may be transmitted from the service server to the payment server through the payment network.

[15] Moreover, user registration in the second method may be made through the card tagging after the interface operating in conjunction with the card issuance
10 agency service is generated in an application of a financial institution.

[16] Furthermore, the user registration in the second method may be made based on an eigenvalue of the user and the virtual code transmitted to the service server through the interface. When a payment is requested through the card for which the registration is completed, the card number of the card may be transmitted from a
15 payment server to the service server through a payment network and may be used to extract the eigenvalue of the user. The eigenvalue of the user may be transmitted to a server of the financial institution and may be used to extract the card number of the mobile card.

[17] Besides, in the receiving, the current time data may be received along with an
20 APDU command for driving the applet, upon the card tagging. In the generating, the applet may be driven and generated depending on the APDU command.

[18] According to an embodiment, a holderless card device having a physical form in a state where a user is not registered includes an NFC module that performs NFC-based communication when tagging a terminal of the user, and an IC module
25 including an applet for generating a virtual code for authentication of the user. The

IC module receives current time data from the user terminal through the NFC module when tagging the user terminal, allows the applet to generate a virtual code based on the current time data and pre-stored seed data, and makes a request for verification of the virtual code to the verification server by transmitting the virtual code to a verification server through the user terminal. When the card device is produced while the user is not registered, and the verification is completed, the card device is connected to a mobile card already owned by the user in the verification server such that the user is registered.

[19] Besides, a computer program stored in a computer-readable recording medium for execution to implement the inventive concept may be further provided.

[20] In addition, a computer-readable recording medium for recording a computer program for performing the method to implement the inventive concept may be further provided.

15 【 ADVANTAGEOUS EFFECTS OF THE INVENTION】

[21] According to the above-mentioned problem solving means of the inventive concept, financial institutions may reduce the cost of producing and delivering physical cards by issuing cards through a linked card manufacturer or by using an external issuance agency service.

20 [22] Moreover, cards may be customized by linking with a card manufacturer or using an external issuance agency service, and physical cards may be used as a new transaction item by using them for marketing.

[23] Furthermore, an annual fee needs to be paid to use a conventional physical card. However, there is no need to pay an annual fee for a physical card by connecting a physical card to a mobile card and using the mobile card.

[24] Effects of the inventive concept are not limited to the effects mentioned above, and other effects not mentioned will be clearly understood by those skilled in the art from the following description.

5 【 DESCRIPTION OF THE DRAWINGS 】

[25] FIG. 1 is a diagram schematically illustrating a system for registering a user in a holderless card by using an authentication virtual code, according to an embodiment of the inventive concept.

[26] FIG. 2 is a schematic block diagram of a holderless card device, according to
10 an embodiment of the inventive concept.

[27] FIG. 3 is a flowchart of a method of registering a user in a holderless card by using an authentication virtual code, according to an embodiment of the inventive concept.

[28] FIG. 4 is a diagram for describing how to register a user by connecting a
15 physical card, in which the user is not registered, to a mobile card, according to an embodiment of the inventive concept.

[29] FIG. 5 is a diagram for describing a registration process when a verification server is a financial institution server, according to an embodiment of the inventive concept.

[30] FIGS. 6 and 7 are diagrams for describing a registration process in the case
20 where a verification server is a service server operating as a card issuing agent, according to an embodiment of the inventive concept.

[31] FIG. 8 is a diagram illustrating a computing device, according to an embodiment of the inventive concept.

25

【 BEST MODE】

[32] The same reference numerals denote the same elements throughout the inventive concept. The inventive concept does not describe all elements of embodiments. Well-known content or redundant content in which embodiments are the same as one another will be omitted in a technical field to which the inventive concept belongs. A term such as ‘unit, module, member, or block’ used in the specification may be implemented with software or hardware. According to embodiments, a plurality of ‘units, modules, members, or blocks’ may be implemented with one component or a single ‘unit, module, member, or block’ may include a plurality of components.

[33] Throughout this specification, when it is supposed that a portion is "connected" to another portion, this includes not only a direct connection, but also an indirect connection. The indirect connection includes being connected through a wireless communication network.

[34] Furthermore, when a portion “comprises” a component, it will be understood that it may further include another component, without excluding other components unless specifically stated otherwise.

[35] Throughout this specification, when it is supposed that a member is located on another member "on", this includes not only the case where one member is in contact with another member but also the case where another member is present between two other members.

[36] Terms such as ‘first’, ‘second’, and the like are used to distinguish one component from another component, and thus the component is not limited by the terms described above.

[37] Unless there are obvious exceptions in the context, a singular form includes a

plural form.

[38] In each step, an identification code is used for convenience of description. The identification code does not describe the order of each step. Unless the context clearly states a specific order, each step may be performed differently from the specified order.

[39] Hereinafter, operating principles and embodiments of the inventive concept will be described with reference to the accompanying drawings.

[40] Hereinafter, an embodiment of the inventive concept will be described in detail with reference to the accompanying drawings.

10 [41] Prior to a description, the meaning of terms used in the present specification will be described briefly. However, because the description of terms is used to help the understanding of this specification, it should be noted that if the inventive concept is not explicitly described as a limiting matter, it is not used in the sense of limiting the technical idea of the inventive concept.

15 [42] In this specification, a “character” is a component constituting a code and includes all or part of uppercase alphabet characters, lowercase alphabet characters, numerals, and special characters.

[43] In this specification, a “code” refers to a string of characters.

[44] In this specification, “authentication virtual code” may mean a one-time authentication code (OTAC) temporarily generated to register a user.

20 [45] In this specification, a “holderless card” is a physical card equipped with an applet for generating a virtual code, and refers to a card produced and issued while a user is not assigned. The holderless card may not have a user assigned to it, but may store an actual card number capable of being used to make a payment after a process
25 of registering a user.

[46] In this specification, a "virtual code generation function" means a function that generates a virtual code. For example, one time password (OTP), etc. are included therein, but are not limited thereto.

[47] In this specification, a 'detailed code generating function' refers to a function
5 of generating each detailed code constituting the virtual code.

[48] In this specification, the "detailed code combination function" refers to a function for generating a virtual code by combining or coupling a plurality of detailed codes.

[49] In this specification, a 'unit count' is a unit set to a specific time interval and
10 is defined to change as the time interval elapses. For example, 1 count may be used after being set to a specific time interval (e.g., 1.5 seconds).

[50] In this specification, a 'storage location' refers to a point (count) on a track corresponding to a point in time when the registration of a card is requested by a user.

15 [51] In this specification, "user registration" and "card registration" may be interpreted in the same meaning as performing registration by assigning a user to a holderless card in a form of a physical form in which the user is not specified.

[52] FIG. 1 is a diagram schematically illustrating a system for registering a user in a holderless card by using an authentication virtual code, according to an
20 embodiment of the inventive concept.

[53] Referring to FIG. 1, a system 1 (hereinafter referred to as a "system") for registering a user in a holderless card by using an authentication virtual code includes a physical card 10, a user terminal 20, and a verification server 30. However, in some embodiments, the system 1 may include fewer or more components than the
25 components illustrated in FIG. 1.

[54] The physical card 10 may be a holderless card manufactured and issued while a user is not specified (registered). Afterwards, when the user registration is completed through virtual code verification, the physical card 10 may be connected to a mobile card already possessed and employed by the user. In this specification, a
5 “physical card” and a “holderless card” may be interpreted as the same meaning as each other.

[55] Because the user is not specified, user-related information is not embedded in the physical card 10 at the time of manufacture. According to an embodiment, no information may be displayed on the surface of the physical card 10.

10 [56] The physical card 10 may include an applet for generating an authentication virtual code, and may generate the authentication virtual code (hereafter referred to as a “virtual code”) based on data received from the user terminal 20 and embedded data by using the applet. In an embodiment of the inventive concept, the physical card 10 may be a card device that performs various calculation processes for card
15 registration by including the applet.

[57] The user terminal 20 may transmit current time data to the physical card 10 when tagging the physical card 10.

[58] The user terminal 20 may receive a virtual code from the physical card 10 and may transmit user information to the verification server 30 together with the
20 virtual code.

[59] The verification server 30 may verify the virtual code received from the user terminal 20. When it is determined that the received virtual code is normally generated at this point, the verification server 30 may complete user registration for the physical card 10. As such, the physical card 10 of the user may be connected to a
25 mobile card that is already employed by a user. After that, when a payment is

requested by using the physical card 10, the payment may be made with the mobile card connected to the physical card 10.

[60] Referring to FIG. 1, the verification server 30 may be shown as being composed of one server, but may be composed of a system in which a plurality of
5 servers are affiliated with each other.

[61] As shown in FIG. 1, the physical card 10, the user terminal 20, and the verification server 30 may transmit and receive various types of data, signals, or information through a communication network.

[62] Here, various types of communication networks may be used. For example,
10 wireless communication methods such as wireless LAN (WLAN), Wi-Fi, Wibro, Wimax, High Speed Downlink Packet Access (HSDPA), and the like or wired communication methods such as Ethernet, xDSL (ADSL or VDSL), Hybrid Fiber Coax (HFC), Fiber to the Curb (FTTC), Fiber to the Home (FTTH), and the like may be used in a communication network.

15 [63] In the meantime, the communication network is not limited to the communication method described above, and may include all types of communication methods widely known or to be developed in the future in addition to the above communication methods.

[64] FIG. 2 is a schematic block diagram of a holderless card device, according to
20 an embodiment of the inventive concept. A holderless card device 100 in FIG. 2 means the physical card 10 described with reference to FIG. 1. In other words, the holderless card device 100 is manufactured while a user is not registered. When virtual code verification is completed, the holderless card device 100 may refer to the physical card 10 in which the user is registered by being connected to a mobile card
25 already possessed by the user in the verification server 30.

[65] Referring to FIG. 2, the holderless card device 100 may include a narrow frequency communication (NFC) module 120 and an IC module 140. However, in some embodiments, the holderless card device 100 may include fewer or more components than the components illustrated in FIG. 2.

5 [66] The NFC module 120 (i.e., an NFC chip) may be a communication module and may perform NFC-based communication when tagging the user terminal 20.

[67] The IC module 140 (i.e., an IC chip) may include an applet for generating a virtual code for authenticating a user. Although the IC module is described as including an applet, the IC module 140 may be an applet itself.

10 [68] In more detail, the IC module 140 may include an EMV applet and an OTAC applet. A card number of the physical card 10 and an eigenvalue of the physical card 10 may be embedded in the EMV applet. Seed data for generating a virtual code (OTAC) may be embedded in the OTAC applet.

[69] When tagging the user terminal 20, the IC module 140 may receive current
15 time data from the user terminal 20 through the NFC module 120, may generate a virtual code based on the current time data and pre-stored seed data by using (controlling) the applet (in particular, the OTAC applet), and may transmit the virtual code to the user terminal 20 through the NFC module 120. The user terminal 20 may transmit the virtual code to the verification server 30 to request verification of the
20 virtual code.

[70] FIG. 2 shows that the holderless card device 100 includes only the NFC module 120. However, the holderless card device 100 may further include a separate communication module to communicate with the user terminal 20. In other words, the virtual code may be transmitted to the user terminal 20 through a separate
25 communication module. Here, the separate communication module may include a

wireless communication module and a short-range communication module.

[71] The wireless communication module may support various wireless communication methods such as Global System for Mobile (GSM) communication, Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Universal Mobile Telecommunication System (UMTS), Time Division Multiple Access (TDMA), Long Term Evolution (LTE), 4G, 5G, and 6G in addition to a wifi module and Wireless broadband module.

[72] The short-range communication may be used for short range communication, and may support short-range communication by using at least one of Bluetooth™, radio frequency identification (RFID), infrared data association (IrDA), ultra wideband (UWB), ZigBee, near field communication (NFC), Wireless-Fidelity (Wi-Fi), Wi-Fi Direct, and wireless universal serial bus (Wireless USB) technologies.

[73] The IC module 140 is mounted on a PCB board to perform data exchange by contacting a terminal of an IC-type card reader. The IC module 140 includes an arbitrary form such as a component including an integrated circuit (IC) and a system on chip (SoC). For example, the IC chip may be of an ISO 14443 NXP Mifare Classic type according to an embodiment of the inventive concept, but is not limited thereto.

[74] FIG. 3 is a flowchart of a method of registering a user in a holderless card by using an authentication virtual code, according to an embodiment of the inventive concept. FIG. 4 is a diagram for describing how to register a user by connecting a physical card, in which the user is not registered, to a mobile card, according to an embodiment of the inventive concept. The method of FIG. 3 may be performed by a holderless card. Hereinafter, although the method of FIG. 3 is described as being performed by the physical card 10 shown in FIG. 1, it may also be understood that

the method of FIG. 3 is performed by the holderless card device 100.

[75] In an embodiment of the inventive concept, when a user wants to use the physical card 10 for an offline payment by connecting the physical card 10 to a mobile card that is already registered and used in a financial institution application (app), user registration of the physical card 10 (holderless card) may be performed. In an embodiment of the inventive concept, the physical card 10 may be obtained by directly purchasing a user, rather than being delivered to the user by a financial institution.

[76] Referring to FIG. 3, the physical card 10 may receive current time data from the user's terminal 20 (hereafter referred to as a "user terminal") through card tagging (S110).

[77] The physical card 10 may generate a virtual code for user authentication based on the current time data and seed data pre-stored in the physical card by using the applet included in the card (S120). At this time, the virtual code generated in each card may be generated so as not to be duplicated between cards by the seed data stored in the card.

[78] The physical card 10 may request verification of the virtual code by transmitting the virtual code to the verification server 30 through the user terminal 20 (S130).

[79] The physical card 10 may receive the current time data together with an APDU command for driving the applet from the user terminal 20 when tagging the card.

[80] That is, when the physical card 10 receives the APDU command and the current time data from the user terminal 20 through card tagging, the physical card 10 may drive an applet based on the APDU command. Moreover, the virtual code

may be generated based on the received current time data and the seed data for generating the virtual code already stored in the card, by using the running applet. The virtual code generated in this way may be transmitted to the user terminal 20.

[81] The user terminal 20 may transmit at least one of user information logged
5 into a financial service application and the received virtual code to the verification server 30. Here, the user information may include login information of a user and mobile card information that the user wants to connect with the physical card 10. Here, the financial service application may be an application built by a financial institution itself, or an application provided from an external server.

10 [82] When it is determined that the virtual code is normally generated at this point, the verification server 30 may connect the physical card 10 to the mobile card to complete user registration for the physical card 10.

[83] Referring to FIG. 3, the physical card 10 may be produced and issued while a user is not registered. The user may purchase the physical card 10, may register the
15 physical card 10 in a financial institution application, and may connect the physical card 10 to the mobile card in use to perform card registration. In more detail, the user may install a financial service application in his/her user terminal 20 and may connect a mobile card already used to the physical card 10 through the corresponding application. In detail, when the verification server 30 completes verification of the
20 virtual code generated by the physical card 10, the corresponding physical card 10 may be connected to the mobile card, and thus a user of the mobile card may be completely registered as a user of the physical card 10. Here, when the financial service application is an application built by a financial institution itself, the user registration may be performed by using one application provided by the financial
25 institution. When the financial service application is an application received from an

external server, the user registration may be performed by using the application provided by the financial institution and an application provided by an external service provider (i.e., two applications).

[84] Hereinafter, a method in which the physical card 10, which operates as a virtual code generating device, generates a virtual code will be described in detail.

[85] The OTAC applet included in the physical card 10 may generate one or more detailed codes. The detailed code means some codes constituting a virtual code. The virtual code may consist of only detailed codes, or may be formed in a form of a final virtual code (OTAC) by combining one or a plurality of detailed codes with a first virtual security code generated by an OTP function.

[86] The OTAC applet includes a virtual code generation function for generating a virtual code. The virtual code generation function includes a detailed code generation function that generates one or more detailed codes, and a detailed code combination function (i.e., a rule for combining a plurality of detailed codes) that generates a virtual code by combining the detailed codes.

[87] That is, when the virtual code includes a plurality of detailed codes. The virtual code generation function generates a plurality of detailed codes by using a plurality of detailed code generation functions, and generates a virtual security code by combining the plurality of detailed codes into a preset combination through the detailed code combination function.

[88] The plurality of detailed codes have a correlation used such that the verification server 30 searches for a storage space of information capable of identifying a user or card. In other words, the verification server 30 includes a search algorithm (a storage space search algorithm). The search algorithm extracts a plurality of detailed codes included in the virtual code, and searches for the storage

space of identification information assigned to the user or card based on the correlation between the plurality of detailed codes. As an embodiment of the correlation between the plurality of detailed codes, the search algorithm included in the verification server 30 may perform a calculation based on the correlation between the plurality of detailed codes from waypoints corresponding to one or more detailed codes among the plurality of detailed codes, and thus may search for a storage location of identification information of the user or card. At this time, there are one or more waypoints, and there is no limit to the number and order.

[89] Furthermore, as an embodiment of a plurality of detailed codes, the plurality of detailed codes may include a first code and a second code. The OTAC applet generates the first code and the second code by including a first function and a second function as detailed code generation functions. The first code and the second code have a correlation for searching for a storage location of the identification information of the user or card within the verification server 30. However, the OTAC applet may include the first function for generating the first code and the second function for generating the second code as detailed code generation functions to improve security, and may not include data for the correlation between the first code and the second code.

[90] As a specific example of the correlation between the first code and the second code, each of the first code and the second code may be used to search for the storage space of the identification information. In other words, the first code may include information about a waypoint. The second code may include information necessary for calculation capable of being reached from the waypoint to the storage location of the identification information.

[91] In the meantime, in an embodiment of the inventive concept, the first code

may be generated based on a first count. The second code may be generated based on a second count. In this case, the first count may include the number of unit counts that have elapsed from a first time point at which the virtual code generation function is driven in the verification server 30 to a time point at which the virtual code is generated. The second count may include the number of unit counts that have elapsed from a time point at which the identification information of the user or card is registered in the verification server 30.

[92] In other words, 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.

[93] Hereinafter, a method in which the verification server 30, which operates as a virtual code verification device, verifies a virtual code will be described in detail.

[94] In an embodiment of the inventive concept, when receiving the virtual code from the user terminal 20, the verification server 30 may verify the virtual code by comparing time data regarding a time point, at which the virtual code is received, and time data of the virtual code.

[95] In detail, the verification server 30 verifies whether the virtual code is normally generated. In other words, after receiving the virtual code, the verification server 30 determines whether the virtual code is normal, by determining whether the received virtual code is normally generated at the present time, based on information (i.e., a virtual code generation function and seed data) stored in the verification server 30. For example, the verification server 30 determines whether there is a value, which matches the virtual code, among OTP numbers calculated by entering counts within a specific range from a count, at which the virtual code is received,

into the virtual code generation function (i.e. An OTP function). The verification server 30 searches for a count corresponding to a time point at which the virtual code is generated, by applying an inverse function of the virtual code generation function to the virtual code. As a difference between a time point at which the virtual code is generated and a time point at which the verification server 30 receives the virtual code is present due to the transmission time of the virtual code or delay, a count at which the verification server 30 receives the virtual code may not be the same as a count at which the OTP number corresponding to the virtual code is generated, and thus the verification server 30 allows an error range from the count at which the virtual code is received.

[96] In the meantime, in an embodiment of the inventive concept, the verification server 30 may extract the identification information of the user or card by searching for the storage location of the identification information of the user or card based on the virtual code, and may perform user authentication based on the extracted identification information.

[97] FIG. 5 is a diagram for describing a registration process when a verification server is a financial institution server, according to an embodiment of the inventive concept. Hereinafter, a user registration process in the case where a financial institution produces and issues the physical card 10 by itself will be described with reference to FIG. 5.

[98] In this case, the verification server 30 becomes the financial institution server 31. The physical card 10 is produced by a card manufacturer affiliated with a financial institution.

[99] In S130, as well as the virtual code, the physical card 10 may further transmit at least one of a card number of the physical card 10 and an eigenvalue of the

physical card 10, which are previously stored in the physical card 10, to the verification server 30 through the user terminal 20.

[100] Moreover, when verification of the virtual code is completed, at least one of the seed data in the verification server 30, the card number of the physical card 10, and the eigenvalue of the physical card 10 may be matched with user information generated by the user terminal 20 and then may be stored.

[101] In more detail, when the verification is completed, the verification server 30 may extract seed data included in the virtual code and may complete user registration for the corresponding physical card 10 by matching at least one of the extracted seed data, the card number of the physical card 10, and the eigenvalue of the physical card 10 with the user information. Here, the user information may include login information of a user logged into a financial institution application, and information (a mobile card number) of a mobile card possessed by the user.

[102] The card number of the physical card 10, the eigenvalue of the physical card 10, and the seed data are transmitted to a server of a card manufacturer by the verification server 30 and are embedded in an IC chip (EMV applet and OTAC applet) when the physical card 10 is manufactured. That is, the card number of the physical card 10, the eigenvalue of the physical card 10, and the seed data of the physical card 10 may be already stored in the verification server 30.

[103] Here, the card number of the physical card 10 may include an identification code (e.g., BIN) of the financial institution. The eigenvalue of the physical card 10 may be a value sequentially assigned to each card manufactured by the card manufacturer. The card manufacturer may install a virtual code (OTAC) server on a WAS server within the financial institution system and may sequentially input the eigenvalue provided by the virtual code (OTAC) server when manufacturing a

physical card.

[104] According to an embodiment, when the physical card 10 transmits the virtual code, the card number of the physical card 10, and the eigenvalue of the physical card 10 to the verification server 30 through the user terminal 20, the verification
5 server 30 may completely verify the virtual code and then may match seed data extracted from the virtual code, the card number of the physical card 10, and the eigenvalue of the physical card 10 with user information so as to be stored.

[105] According to an embodiment, when the physical card 10 transmits the virtual code and the card number of the physical card 10 to the verification server 30
10 through the user terminal 20, the verification server 30 may completely verify the virtual code and then may match seed data extracted from the virtual code and the card number of the physical card 10 with the user information so as to be stored.

[106] According to an embodiment, when the physical card 10 transmits the virtual code and the eigenvalue of the physical card 10 to the verification server 30 through
15 the user terminal 20, the verification server 30 may completely verify the virtual code and then may match seed data extracted from the virtual code and the eigenvalue of the physical card 10 with the user information so as to be stored.

[107] According to an embodiment, when the physical card 10 transmits first information (e.g., a card number) among the virtual code, the card number of the
20 physical card 10, and the eigenvalue of the physical card 10 to the verification server 30 through the user terminal 20, the verification server 30 may completely verify the virtual code, may extract seed data from the virtual code, may extract second information (e.g., an eigenvalue) from the received first information (e.g., a card number) among the card number and the eigenvalue of the physical card 10, and may
25 match the extracted seed data, the extracted second information (e.g., an eigenvalue),

the received first information (e.g., a card number), and received user information so as to be stored.

[108] Referring to FIG. 5, when tagging is made between the physical card 10 and the user terminal 20, the user terminal 20 may transmit current time data to the physical card 10 (S21). The physical card 10 may generate a virtual code based on the received current time data and pre-stored seed data (S22). The physical card 10 may transmit at least one of the generated virtual code, the pre-stored card number of the physical card 10, and the pre-stored eigenvalue of the physical card 10 to the user terminal 20 (S23). The user terminal 20 transmits user information to the financial institution server 31 together with at least one of the received virtual code, the card number of the physical card 10, and the eigenvalue of the physical card 10 (S24). The financial institution server 31 may perform verification to determine whether the virtual code is a normally generated code at this time (S25). When it is determined that the virtual code is a normal code (when the verification is completed), the financial institution server 31 may complete user registration for the physical card 10 by matching at least one of the seed data, the card number of the card, and the eigenvalue of the card, with user information (S26).

[109] Accordingly, the physical card 10 and the mobile card are connected to each other within the financial institution server 31. Afterward, when a user requests an offline payment by using the physical card 10, a payment may be made by using the mobile card connected to the physical card 10. Here, the physical card 10 and the mobile card may be connected by matching and storing the physical card number and the mobile card number in the financial institution server 31.

[110] FIGS. 6 and 7 are diagrams for describing a registration process in the case where a verification server is a service server operating as a card issuing agent,

according to an embodiment of the inventive concept. Hereinafter, a process of registering a user in the case where a financial institution uses the physical card 10 produced externally will be described with reference to FIGS. 6 and 7. The reason that financial institutions use externally produced physical cards without producing their own physical cards is that the financial institutions need a service capable issuing a physical card to users while reducing related costs (physical card production and shipping cost) because the number of physical cards capable of being used offline is decreasing nowadays, and physical cards and mobile car /mobile payments are coexisting.

10 [111] When the physical card 10 produced by a service provider operating as an agent for card issuance is used, the verification server 30 becomes a service server 32 (hereinafter referred to as a “service server”) operating as an agent for card issuance, and the physical card 10 is produced by a provider of a card issuance agency service.

[112] When the physical card 10 manufactured by the service provider is used, user registration may be made in an application-based first method for physical card registration or an interface-based second method for physical card registration.

15 [113] - User Registration Method when User Registration is performed in First Method

[114] The user terminal 20 may be provided with a registration application provided by the service server 32.

20 [115] After a card number of a mobile card already owned by a user is entered through the registration application, user registration in the first method may be made through tagging between the physical card 10 and the user terminal 20.

[116] Here, user registration in the first method may be made by matching the card number of the physical card 10 found by the service server 32 based on the virtual

25

code with the card number of the mobile card.

[117] Afterward, when the user requests a payment by using the registered physical card 10, the card number of the physical card 10 may be transmitted from a payment server (not shown) to the service server 32 through a payment network, and the card
5 number of the mobile card matched to the card number of the physical card 10 may be transmitted from the service server 32 to the payment server through the payment network.

[118] In this case, the service server 32 may bill the financial institution depending on the number of payments made by using the physical card 10 (a physical card
10 number) and the number of users who employ the physical card 10 issued through a card issuance agency service.

[119] Referring to FIG. 6, the service server 32 may provide an application for registration to the user terminal 20 (S31). The user terminal 20 may install an application for registration (S32). The user may enter the card number of the mobile
15 card, which he/she is employing, through the application for registration (S33). Next, when tagging is made between the physical card 10 and the user terminal 20, the user terminal 20 may transmit current time data to the physical card 10 (S34). The physical card 10 may generate a virtual code based on the received current time data and pre-stored seed data (S35). The physical card 10 may transmit the generated
20 virtual code to the user terminal 20 (S36). The user terminal 20 may transmit the virtual code and the card number of the mobile card, which is entered by the user, to the service server 32 (S37). The service server 32 may search for the card number of the physical card 10 based on the virtual code (S38). In particular, the issuance agent server 32 may extract seed data included in the virtual code and may search for a
25 physical card number that is stored in the server after being matched with the seed

data. The service server 32 may complete user registration by matching the found card number of the physical card with the card number of the mobile card (S39).

[120] Accordingly, when the user requests an offline payment by using the physical card 10, the service server 32 may receive a card number of a physical card from a payment server (not shown) through a payment network. The service server 32 may provide the card number (a mobile card number) of the mobile card matched to the received card number (a physical card number) of the physical card to the payment server through the payment network such that the payment server makes a payment by using the mobile card number.

10 [121] - User Registration Method when User Registration is performed in Second Method

[122] A registration interface operating in conjunction with the card issuance agency service may be generated in a financial institution application installed in the user terminal 20. Afterward, when the physical card 10 is tagged on the user terminal 20, user registration in the second method may be made through the registration interface. At this time, the registration interface may be generated through the interlocking between SDK and API of the service server 32.

[123] Here, user registration in the second method may be made based on an eigenvalue of a user and the virtual code transmitted to the service server 32 through the registration interface.

[124] Afterward, when the card number (a physical card number) of the physical card 10 is transmitted from the payment server (not shown) to the service server 32 through the payment network in the case where the user requests a payment by using the registered physical card 10, the service server 32 may extract the eigenvalue of the user by using the received physical card number. The service server 32 may

transmit the user's eigenvalue to the financial institution server based on the extracted eigenvalue of the user and financial institution information. The financial institution server may make a payment by searching for the card number (a mobile card number) of the mobile card issued to the user by using the user's eigenvalue.

5 Here, the eigenvalue of the user may mean the user's identification information for a specific mobile card for which the connection with the physical card 10 is requested.

[125] In this case, the service server 32 may bill the financial institution depending on the number of payments made by using the physical card 10 and the number of users who employ the physical card 10 issued through a card issuance agency

10 service.

[126] Referring to FIG. 7, a registration interface operating in conjunction with the service server 32 may be generated in the financial institution application installed in the user terminal 20 (S41). In this case, the registration interface may be generated when a user selects a specific mobile card, which the user wants to connect with the

15 actual card 10, from among mobile cards registered in the financial institution application. Next, when tagging is made between the physical card 10 and the user terminal 20, the user terminal 20 may transmit current time data to the physical card 10 (S42). The physical card 10 may generate a virtual code based on the received current time data and pre-stored seed data (S43). The physical card 10 may transmit

20 the generated virtual code to the user terminal 20 (S44). The user terminal 20 may transmit the virtual code and the eigenvalue of the user to the service server 32 (S45). Here, the eigenvalue of the user may mean user identification information for the specific mobile card. The service server 32 may search for the card number (a physical card number) of the physical card 10 based on the virtual code (S46). In

25 particular, the service server 32 may extract seed data included in the virtual code,

and may search for a physical card number that is stored in the server after being matched with the seed data. The service server 32 may complete user registration by matching the found card number of the physical card with the eigenvalue of the user (S47).

5 [127] Accordingly, when the user requests an offline payment by using the physical card 10, the service server 32 may receive a card number of a physical card from a payment server (not shown) through a payment network. The service server 32 may transmit the eigenvalue of the user to the corresponding financial institution server by using financial institution information and the user's eigenvalue matched to the
10 received card number (a physical card number) of the physical card. The financial institution server may make a payment by searching for the card number of the mobile card connected to the corresponding actual card 10 by using the received eigenvalue of the user.

[128] FIGS. 3 and 5 to 7 illustrate that operations are performed sequentially.
15 However, this is merely illustrative of the technical idea of the inventive concept. Those skilled in the art to which an embodiment of the inventive concept belongs may apply various modifications and variations by changing and performing the order illustrated in FIGS. 3 and 5 to 7 or performing operations in parallel without departing from the essential characteristics of an embodiment of the inventive
20 concept. The embodiment in FIGS. 3 and 5 to 7 is not limited to a time-series order.

[129] In the meantime, in the above description, operations in FIGS. 3 and 5 to 7 may be further divided into additional operations or may be combined into fewer operations, according to an embodiment of the inventive concept. In addition, some operations may be omitted as necessary, and the order between operations may be
25 changed.

[130]

[131] FIG. 8 is a diagram illustrating a computing device, according to an embodiment of the inventive concept. A computing device TN100 may be a device (e.g., the user terminal 20, the verification server 30, or the like) described in this specification.

[132] The computing device TN100 may include at least one processor TN110, a transmission/reception device TN120, and a memory TN130. Moreover, the computing device TN100 may further include a storage device TN140, an input interface device TN150, an output interface device TN160, and the like. The components included in computing device TN100 may be connected by a bus TN170 so as to communicate with one another.

[133] The processor TN110 may execute a program command stored in at least one of the memory TN130 and the storage device TN140. The processor TN110 may be a central processing unit (CPU), a graphics processing unit (GPU), or a dedicated processor performing methods according to an embodiment of the inventive concept. The processor TN110 may be configured to implement procedures, functions, and methods described in relation to an embodiment of the inventive concept. The processor TN110 may control each component of the computing device TN100.

[134] Each of the memory TN130 and the storage device TN140 may store various pieces of information related to the operation of the processor TN110. Each of the memory TN130 and the storage device TN140 may be implemented with at least one of a volatile storage medium and a nonvolatile storage medium. For example, the memory TN130 may be implemented with at least one of a read only memory (ROM) and a random access memory (RAM).

[135] The transmission/reception device TN120 may transmit or receive wired or

wireless signals. The transmission/reception device TN120 may perform communication by being connected to a network.

[136]

[137] Meanwhile, the disclosed embodiments may be implemented in a form of a recording medium storing instructions executable by a computer. The instructions may be stored in a form of program codes, and, when executed by a processor, generate a program module to perform operations of the disclosed embodiments. The recording medium may be implemented as a computer-readable recording medium.

[138] The computer-readable recording medium may include all kinds of recording media in which instructions capable of being decoded by a computer are stored. For example, there may be read only memory (ROM), random access memory (RAM), magnetic tape, magnetic disk, flash memory, optical data storage device, and the like.

[139] Disclosed embodiments are described above with reference to the accompanying drawings. One ordinary skilled in the art to which the inventive concept belongs will understand that the inventive concept may be practiced in forms other than the disclosed embodiments without altering the technical ideas or essential features of the inventive concept. The disclosed embodiments are examples and should not be construed as limited thereto.

CLAIMS

[Claim 1] A method, which is performed by a holderless card having a physical form in a state where a user is not registered and which is used to register
5 the user in the holderless card by using an authentication virtual code, the method comprising:

receiving current time data from a terminal of the user through card tagging;
generating a virtual code for authenticating the user based on the current
time data and pre-stored seed data by using an applet included in the card; and
10 requesting verification of the virtual code by transmitting the virtual code to
a verification server through the user terminal,
wherein, when the card is produced while the user is not registered, and the
verification is completed, the card is connected to the mobile card already owned by
the user in the verification server such that the user is registered.

15

[Claim 2] The method of claim 1, wherein, when the verification server
is a server of a financial institution and the card is produced by a card manufacturer
affiliated with the financial institution, the requesting of the verification includes:

requesting the verification by further transmitting at least one of a pre-stored
20 card number of the card and a pre-stored eigenvalue of the card to the verification
server through the user terminal, and

wherein, when the verification is completed, at least one of the seed data, the
card number of the card, and the eigenvalue of the card is matched with user
information generated by the user terminal in the verification server so as to be
25 stored.

[Claim 3] The method of claim 2, wherein the card number of the card, the eigenvalue of the card, and the seed data are delivered by the verification server to a server of the card manufacturer and are embedded in an IC chip when the card is
5 manufactured,

wherein the card number of the card includes an identification code of the financial institution, and

wherein the eigenvalue of the card is a value sequentially assigned to each card manufactured by the card manufacturer.

10

[Claim 4] The method of claim 1, wherein, when the verification server is a service server providing a card issuance agency service, and the card is produced by a provider of the card issuance agency service, the user is registered in a first method based on an application for physical card registration or a second method
15 based on an interface for physical card registration.

[Claim 5] The method of claim 4, wherein the user terminal is equipped with the application provided by the service server, and

wherein user registration in the first method is made through the card
20 tagging after a card number of the mobile card is entered through the application.

[Claim 6] The method of claim 5, wherein the user registration in the first method is made by the service server by matching a card number of the card found based on the virtual code with the card number of the mobile card,
25 wherein the card number of the card is transmitted from a payment server to

the service server through a payment network when a payment is requested through the card for which the registration is completed, and

wherein the card number of the mobile card matched to the card number of the card is transmitted from the service server to the payment server through the
5 payment network.

[Claim 7] The method of claim 4, wherein user registration in the second method is made through the card tagging after the interface operating in conjunction with the card issuance agency service is generated in an application of a financial
10 institution.

[Claim 8] The method of claim 7, wherein the user registration in the second method is made based on an eigenvalue of the user and the virtual code transmitted to the service server through the interface,
15 wherein, when a payment is requested through the card for which the registration is completed, the card number of the card is transmitted from a payment server to the service server through a payment network and is used to extract the eigenvalue of the user, and

wherein the eigenvalue of the user is transmitted to a server of the financial
20 institution and is used to extract the card number of the mobile card.

[Claim 9] The method of claim 1, wherein, in the receiving, the current time data is received along with an APDU command for driving the applet, upon the card tagging, and
25 wherein, in the generating, the applet is driven and generated depending on

the APDU command.

[Claim 10] A computer program coupled with a computer and stored in a computer-readable recording medium to perform the method of claim 1.

5

[Claim 11] A holderless card device having a physical form in a state where a user is not registered, the holderless card device comprising:

an NFC module configured to perform NFC-based communication when tagging a terminal of the user; and

10 an IC module including an applet for generating a virtual code for authentication of the user,

wherein the IC module is configured to:

when tagging the user terminal, receive current time data from the user terminal through the NFC module;

15 allow the applet to generate the virtual code based on the current time data and pre-stored seed data; and

make a request for verification of the virtual code to the verification server by transmitting the virtual code to a verification server through the user terminal, and

wherein, when the card device is produced while the user is not registered,

20 and the verification is completed, the card device is connected to a mobile card already owned by the user in the verification server such that the user is registered.