

【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:

 a first code which sets a starting point of a search of a storage location of the user
20 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】

 A program stored in a recording medium readable by a computer to execute a
25 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