

【CLAIMS】**【Claim 1】**

A method performed by a device for generating a virtual code for authentication, comprising:

5 transmitting time data to a card upon tagging of the card in which an IC chip has been embedded;

 receiving, from the card, a virtual code for primary authentication generated based on the time data;

 generating a virtual code for secondary authentication by using the virtual code for
10 primary authentication;

 transmitting at least one of the virtual code for primary authentication and the virtual code for secondary authentication to a server; and

 requesting the server to perform verification on the at least one of the virtual code for primary authentication and the virtual code for secondary authentication;

15 wherein the virtual code for primary authentication comprises:

 a first code that is generated based on the time data and a first OTP, and

 a second code that is generated by excluding, from the first code, a first user identification (UID) which is identification information of the card.

【Claim 2】

20 The method of claim 1, wherein generating the virtual code for secondary authentication comprises:

 generating a third code by excluding, from the first code, second UID, that is, identification information of the device for generating a virtual code for authentication, and

 generating the virtual code for secondary authentication by combining the first code,
25 the second code, and the third code.

【Claim 3】

The method of claim 2, wherein:

verification is performed on the card based on the first code and the second code, and

verification is performed on the device for generating a virtual code for authentication

5 based on the first code and the third code.

【Claim 4】

The method of claim 1, wherein generating the virtual code for secondary authentication comprises:

generating a second OTP based on the virtual code for primary authentication, and

10 generating the virtual code for secondary authentication based on the second OTP and second UID which is identification information of the device for generating a virtual code for authentication.

【Claim 5】

The method of claim 4, wherein:

15 the virtual code for secondary authentication is verified by comparing the second OTP included in the virtual code for secondary authentication and a second OTP for verification, and

the second OTP for verification is generated by the server based on seed data identical with seed data used when the second OTP is generated.

20 **【Claim 6】**

The method of claim 1, wherein the virtual code for primary authentication is used for user authentication upon offline access control and online login.

【Claim 7】

The method of claim 1, wherein the virtual code for secondary authentication is used
25 for user authentication upon financial settlement.

【Claim 8】

The method of claim 1, wherein the time data has a form combined with an application protocol data unit (APDU) command.

【Claim 9】

5 A program stored in a computer-readable recording medium in order to execute any one method of claims 1 to 8 in combination with a computer.

【Claim 10】

A smart card device comprising:

an NFC module configured to receive time data from a device for generating a virtual
10 code for authentication through card tagging; and

an IC module configured to generate a virtual code for primary authentication based on the received time data,

wherein the virtual code for primary authentication is autonomously transmitted and used for user authentication or is used to generate a virtual code for secondary authentication,

15 the virtual code for secondary authentication is generated by the device for generating a virtual code for authentication by using the virtual code for primary authentication, and

at least one of the virtual code for primary authentication and the virtual code for secondary authentication is transmitted from the device for generating a virtual code for authentication to a server so that the server performs verification on the virtual code for
20 primary authentication and the virtual code for secondary authentication;

wherein the virtual code for primary authentication comprises:

a first code that is generated based on the time data and a first OTP, and

a second code that is generated by excluding, from the first code, a first user identification (UID) which is identification information of the card.

25 **【Claim 11】**

A device for generating a virtual code for authentication, comprising:

a communication unit configured to transmit time data to a card upon tagging of the card in which an IC chip has been embedded and receive, from the card, a virtual code for primary authentication generated based on the time data;

5 a code generation unit configured to generate a virtual code for secondary authentication by using the virtual code for primary authentication; and

a verification request unit configured to request the server to perform verification on at least one of the virtual code for primary authentication and the virtual code for secondary authentication by transmitting the at least one of the virtual code for primary authentication and the virtual code for secondary authentication to the server through the communication unit;

wherein the virtual code for primary authentication comprises:

a first code that is generated based on the time data and a first OTP, and

a second code that is generated by excluding, from the first code, a first user identification (UID) which is identification information of the card.

【Claim 12】

A server for verifying a virtual code for authentication in a method performed by a server, comprising:

receiving at least one of a virtual code for primary authentication and a virtual code for secondary authentication from a device for generating a virtual code for authentication; and

performing verification on at least one of the virtual code for primary authentication and the virtual code for secondary authentication,

wherein if the virtual code for secondary authentication comprises a plurality of codes, performing the verification comprises:

extracting first user identification (UID) which is identification information of a card based on a first code and second code of the plurality of codes and performing verification on the card, and

5 extracting second UID which is identification information of the device for generating a virtual code for authentication based on the first code and third code of the plurality of codes and performing verification on the device for generating a virtual code for authentication.

【Claim 13】

The server of claim 12, wherein if the virtual code for secondary authentication
10 comprises a second OTP and the second UID, performing the verification comprises:

generating a second OTP for verification based on seed data identical with seed data used when the second OTP is generated,

comparing the second OTP included in the virtual code for secondary authentication and the second OTP for verification, and

15 completing the verification on the card and the device for generating a virtual code for authentication when the second OTP and the second OTP for verification are identical with each other.

【Claim 14】

The server of claim 12, wherein when the virtual code for primary authentication is
20 received, performing the verification comprises

extracting the first user identification (UID) which is the identification information of the card based on the virtual code for primary authentication and performing the verification on the card by using a first verification algorithm.