

CLAIMS

1. A user authentication method by using an authentication virtual code,
the method comprising:
 - 5 receiving, by a virtual code verifying means, the authentication virtual code,
wherein the authentication virtual code is generated by an authentication virtual code
generating function included in a virtual code generating means registered in the
virtual code verifying means;
searching, by the virtual code verifying means, for a storage location of user
10 identification (UID) or sub-identification (SID) based on the authentication virtual
code;
extracting, by the virtual code verifying means, authority information stored
after matching the found UID or SID;
verifying, by the virtual code verifying means, the authentication virtual code
15 based on a time point at which the authentication virtual code is received;
wherein, when a time point at which the authentication virtual code is
generated is included in an error range from a time point at which the
authentication virtual code is received, determining, by the virtual code
verifying means, the authentication virtual code as a normal code;
20 wherein, in a state where accessible time information is matched and
stored in the storage location of the UID or the SID, when the time point at
which the authentication virtual code is received belongs to a time zone
corresponding to the accessible time information, determining, by the virtual
code verifying means, the authentication virtual code as the normal code; and
25 performing, by the virtual code verifying means, user authentication based on

the extracted authority information.

2. The method of claim 1, wherein the receiving includes:
generating, by the virtual code generating means, the authentication virtual
5 code;
transmitting, by the virtual code generating means, the generated
authentication virtual code to a virtual code receiving means; and
receiving, by the virtual code verifying means, the authentication virtual code
from the virtual code receiving means.

10

3. The method of claim 2, further comprising:
before receiving the authentication virtual code, transmitting, by the virtual
code generating means, accessible time information matched with the UID or the SID
to the virtual code verifying means; and
15 matching and storing, by the virtual code verifying means, the received
accessible time information with the UID or the SID.

4. The method of claim 3, wherein the performing includes:
extracting, by the virtual code verifying means, the accessible time
20 information stored after matching the storage location of the UID or the SID, and
wherein, only when the authentication virtual code is received within a time
range corresponding to the extracted accessible time information, the virtual code
verifying means performs the user authentication.

25 5. The method of claim 1, wherein the performing includes:

extracting, by the virtual code verifying means, the UID from the authentication virtual code; and

when the authentication virtual code is the verified authentication virtual code, performing the user authentication regardless of authority information stored after
5 matching the storage location of the extracted UID.

6. The method of claim 2, further comprising:

before receiving the authentication virtual code, transmitting, by the virtual code generating means, a type of access authority matched with the UID or the SID to
10 the virtual code verifying means; and

matching and storing, by the virtual code verifying means, the received type of the access authority with the UID or the SID.

7. The method of claim 6, wherein the performing includes:

15 extracting, by the virtual code verifying means, the type of the access authority stored after matching the storage location of the UID or the SID, and

wherein the virtual code verifying means performs the user authentication corresponding to the type of the access authority by using the authentication virtual code.

20

8. A user authentication program by using an authentication virtual code, the program being stored in a medium in combination with a computer, which is hardware, to perform a method of one of claims 1 to 7.

25 9. An authentication virtual code generating device for user authentication

comprising:

a detailed code generating unit configured to generate one or more detailed codes based on UID or SID registered in the virtual code generating device;

5 a virtual code generating unit configured to generate an authentication virtual code obtained by combining the one or more detailed codes, by using an authentication virtual code generating function; and

an authentication virtual code providing unit configured to transmit the generated authentication virtual code to a virtual code receiving device so as to perform the user authentication on a virtual code verifying device through a virtual
10 code receiving means,

wherein, when a time point at which the authentication virtual code is generated is included in an error range from a time point at which the authentication virtual code is received, determining, by a virtual code verifying means, the authentication virtual code as a normal code; and,

15 wherein, in a state where accessible time information is matched and stored in the storage location of the UID or the SID, when the time point at which the authentication virtual code is received belongs to a time zone corresponding to the accessible time information, determining, by the virtual code verifying means, the authentication virtual code as the normal code.

20

10. An authentication virtual code verifying device for user authentication comprising:

a virtual code receiving unit configured to receive an authentication virtual code;

25 a detailed code extracting unit configured to extract a detailed code from the

authentication virtual code;

a storage location search unit configured to search for a storage location of UID or SID based on the detailed code;

an authority information extracting unit configured to extract authority
5 information stored after matching the found UID or SID;

a virtual code verifying unit configured to verify the authentication virtual code based on a time point at which the authentication virtual code is received,

wherein, when a time point at which the authentication virtual code is generated is included in an error range from a time point at which the authentication virtual code is received, determining, by the virtual code
10 verifying unit, the authentication virtual code as a normal code; and,

wherein, in a state where accessible time information is matched and stored in the storage location of the UID or the SID, when the time point at which the authentication virtual code is received belongs to a time zone
15 corresponding to the accessible time information, determining, by the virtual code verifying unit, the authentication virtual code as the normal code; and

a user authentication approving unit configured to perform the user authentication based on the extracted authority information.

20 11. The authentication virtual code verifying device of claim 10, wherein the authentication virtual code verifying device includes a vehicle or a door lock.

12. The authentication virtual code verifying device of claim 11, wherein, when the authentication virtual code verifying device is the vehicle, the authentication
25 virtual code verifying device receives the UID or the SID and a type of access authority

matched with the UID or the SID from a virtual code generating device and matches and stores the type of the access authority with the UID or the SID, and

wherein the type of the access authority includes in-vehicle access authority, vehicle starting authority, and vehicle driving authority.

5

13. The authentication virtual code verifying device of claim 12, wherein the user authentication approving unit extracts the type of the access authority stored after matching the storage location of the UID or the SID and performs the user authentication by granting one of the in-vehicle access authority, the vehicle starting
10 authority, and the vehicle driving authority depending on the extracted type of the access authority.