

SPECIFICATION

TITLE OF INVENTION

AUTHENTICATION CODE ISSUANCE SYSTEM, AUTHENTICATION
5 CODE ISSUANCE METHOD, TERMINAL DEVICE, AND AUTHENTICATION
CODE UTILIZATION METHOD

TECHNICAL FIELD

[0001]

10 The present invention relates to an authentication code issuance system, an
authentication code issuance method, a terminal device, an authentication code
utilization method, and the like.

BACKGROUND ART

[0002]

15 In recent years, illegal use represented by so-called spoofing has been
increasing rapidly in services such as Internet banking services and online stores via the
world wide web (WWW).

[0003]

20 Recently, a configuration of a system for the above services has been proposed
in which the authenticity of a supplier or a client is determined using location
information of the supplier or the client, and an approval process of approving the
electronic commerce is executed (for example, Japanese Patent No. 7321418).

SUMMARY OF THE INVENTION

25 PROBLEM TO BE SOLVED BY THE INVENTION

[0004]

However, in the system of Patent Document 1, there is room for improvement regarding the conflicting objects and effects of identity authentication and the securing anonymity while taking into consideration the acquisition of personal information when the approval process is performed.

5 [0005]

The present invention has been made to address the above-mentioned issues, and the object of the present invention is to provide an authentication code issuance system capable of issuing an authentication code in which reliability as identity authentication is secured while anonymity is secured by a simple configuration.

10 [0006]

Also, the present invention has been made to address the above-mentioned issues, and an object of the present invention is to provide a terminal device which is highly reliable by using an authentication code having such characteristics with the securing anonymity, and which can realize various activities such as economic activities of a user in a virtual space using a network service in a manner comparable to that in real space.

SOLUTION TO THE PROBLEM

[0007]

20 (1) An authentication code issuance system according to a first aspect of the present invention is an authentication code issuance system for issuing a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the system having a configuration including:

25 a virtual identification information acquisition unit for acquiring the identification information of the user in the virtual space as virtual identification information;

a location information acquisition unit for acquiring, from a terminal device held by the user, current location information indicating a current location of the terminal device and time information indicating a time at which the current location is identified;

5 an authentication code issuance unit for issuing a non-fungible authentication code for identity verification for using a given network service, the authentication code being a code of identification information unique to the user, by associating the acquired virtual identification information with the acquired current location information and time information as the entity information; and

10 a registration unit for registering the issued authentication code in a given database after assigning the issued authentication code to the user.

[0008]

(2) Also, a terminal device according to a second aspect of the present invention is a terminal device utilizing a unique authentication code in which

15 identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the terminal device having a configuration including:

a receiving unit for receiving the identification information of the user in the virtual space as virtual identification information;

20 an identification unit for identifying a current location and a time at which the current location is identified;

a requesting unit for requesting a server system to issue a non-fungible authentication code for identity verification for using a given network service, by associating the received virtual identification information with current location

25 information indicating the identified current location and time information indicating the time at which the current location is identified as the entity information; and

a service-related process execution unit for executing a service-related process associated with the network service using the authentication code that is issued based on an issuance request and registered in a given database after being assigned to the user.

[0009]

5 (3) Also, an authentication code utilization method according to a third aspect of the present invention is an authentication code utilization method for utilizing a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the method having a configuration including:

10 receiving the identification information of the user in the virtual space as virtual identification information;

 identifying a current location and a time at which the current location is identified;

 requesting a server system to issue a non-fungible authentication code for
15 identity verification for using a given network service, by associating the received virtual identification information with current location information indicating the identified current location and time information indicating the time at which the current location is identified as the entity information; and

 executing a service-related process associated with the network service using
20 the authentication code that is issued based on an issuance request and registered in a given database after being assigned to the user.

[0010]

 (4) Also, an authentication code issuance method according to a fourth aspect of the present invention is an authentication code issuance method for issuing a unique
25 authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the method having a configuration including:

acquiring identification information of the user in the virtual space as virtual identification information;

acquiring, from a terminal device held by the user, current location information indicating a current location of the terminal device and time information indicating a
5 time at which the current location is identified;

issuing a non-fungible authentication code for identity verification for using a given network service, the authentication code being a code of identification information unique to the user, by associating the acquired virtual identification information with the acquired current location information and time information as the
10 entity information; and

registering the issued authentication code in a given database after assigning the issued authentication code to the user.

BRIEF DESCRIPTION OF DRAWINGS

15 [0011]

Fig. 1 is a system configuration diagram illustrating a network-based identity authentication system according to an embodiment.

Fig. 2 is one example of a diagram illustrating functional blocks of the token issuance server of the present embodiment.

20 Fig. 3 is a functional block diagram illustrating an example of a configuration of a terminal device according to the embodiment.

Fig. 4 is a diagram for explaining an authentication code issuance process executed in the token issuance server and an authentication code issuance request process executed by the terminal device according to the embodiment.

25 Fig. 5 is a flowchart illustrating an operation of the authentication code issuance request process executed by the terminal device according to the embodiment.

Fig. 6 is a flowchart illustrating the operation of the authentication code issuance request process executed by the terminal device according to the embodiment.

Fig. 7 is a flowchart illustrating an operation of the authentication code issuance process executed by the token issuance server according to the embodiment.

5 Fig. 8 is a system configuration diagram illustrating a configuration of the network-based identity authentication system in a second modification of the embodiment.

Fig. 9 is a diagram for explaining a motion capture process of a user executed in an information processing server in the second modification of the embodiment.

10 Fig. 10 is a diagram for explaining a motion capture process of the user executed in the token issuance server in the second modification of an embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENT

[0012]

15 (1) An embodiment of the present invention has a configuration of a network-based identity authentication system that issues a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user actually exists in real space, the system including:

a virtual identification information acquisition unit for acquiring the
20 identification information of the user in the virtual space as virtual identification information;

a location information acquisition unit for acquiring, from a terminal device of the user, current location information indicating a current location of the terminal device and time information indicating a time at which the current location is identified;

25 an authentication code issuance unit for issuing a non-fungible authentication code for identity verification to be used for a given network service, the authentication code being a code of the user's unique identification information, by associating the

acquired virtual identification information with the acquired current location information and time information as the entity information; and

a registration unit for registering the issued authentication code in a given database after assigning the issued authentication code to the user.

5 [0013]

Based on this configuration, an embodiment of the present invention can associate identification information (i.e., ID) in virtual space with information for proving an entity in real space via the authentication code. Accordingly, even for user activities in the virtual space, the actual existence can be ensured by using the authentication code.

[0014]

Specifically, the embodiment of the present invention can issue the authentication code for which the reliability of identity authentication is ensured while maintaining anonymity. Accordingly, it is possible to realize various activities such as economic activities of the user in the virtual space using network services, while ensuring both anonymity and high reliability for identity authentication.

[0015]

The "non-fungible authentication code for identity verification" may be, for example, a non-transferable token such as an SBT (Soul Bound Token), or may be a digital code like a digital certificate.

[0016]

The phrase "assigning the authentication code to the user" indicates that, while being usable on the network, the authentication code is non-transferable to others.

[0017]

25 (2) The embodiment of the present invention has a configuration including the authentication code issuance unit that issues the authentication code having a limited period of use.

[0018]

Based on this configuration, the embodiment of the present invention can render the authentication code unusable within a short period after issuance of the authentication code, such as one hour or one day. Accordingly, each time the authentication code is issued, the latest location of the user can be recognized, and as a result, it is possible to periodically recognize whether the user actually exists.

[0019]

Furthermore, the embodiment of the present invention can determine whether a range of activity of the user is appropriate or whether identity verification is continuously performed by tracing the location of the user or a part of the user's body. Accordingly, it is possible to prove the authenticity of the user or continuously prove the authenticity of the user.

[0020]

(3) The embodiment of the present invention has a configuration including the registration unit that encrypts the authentication code and registers the encrypted authentication code in a plurality of the databases on a network in a distributed manner.

[0021]

Based on this configuration, the embodiment of the present invention can register the authentication code in a plurality of the databases by using a distributed ledger technology such as a blockchain which is difficult to be falsified, and therefore can improve the reliability of identity authentication.

[0022]

The phrase "registering the encrypted authentication code in a plurality of the databases on the network in a distributed manner" indicates that the encrypted authentication code is managed in a distributed manner by using, for example, a blockchain technology to prevent falsification, rather than being managed in a centralized manner.

[0023]

(4) The embodiment of the present invention has a configuration including the authentication code issuance unit that issues the authentication code for identity verification by using at least the current location information as biometric information of the user.

[0024]

Based on this configuration, the embodiment of the present invention can accurately perform identity authentication by using the current location information.

[0025]

The phrase "using as biometric information of the user" includes not only the location of the user itself but also, for example, recognizing a characteristic movement (motion) of the user by using the location information and using the recognized movement of the user as biometric information.

[0026]

(5) The embodiment of the present invention has a configuration including an information management unit for managing user information regarding a user corresponding to each of the users stored in a storage unit, the user information being motion feature information that indicates a feature of movement of a part of a body of the user; and

the authentication code issuance unit that:

detects a trajectory of the part of the body of the user as part trajectory information based on a plurality of the current location information, and identifies motion information indicating a physical movement of the user based on the detected part trajectory information;

executes a determination process of determining identity of the movement of the physical part of a target user based on the motion feature information

of the target user who requested issuance of the authentication code and the identified motion information;

executes an authentication process of performing identity authentication of the target user when it is determined in the determination process that the movement of the part indicated by the motion feature information and the movement of the physical part of the target user indicated by the motion information are movements that are the same or are regarded as being the same; and

issues the authentication code for identity verification when the identity authentication by the authentication process is successful.

10 [0027]

Based on this configuration, the embodiment of the present invention can recognize a characteristic movement (motion) of the user by using the location information and use the recognized movement of the user as biometric information, and therefore can issue the authentication code for the identity authentication for which reliability is ensured while ensuring anonymity.

[0028]

Therefore, the embodiment of the present invention can realize various activities such as economic activities of the user in a virtual space using network services while ensuring anonymity and having high reliability for identity authentication.

[0029]

The phrase "motion feature information" indicates feature information regarding movement of a physical part, and indicates, for example, a range of motion of limbs, head, or upper body, or left-right differences, or irregular movements or part locations such as habits.

[0030]

The phrase "a part of a body of the user" includes, for example, wrists, ankles, the top of the head, the forehead, elbows, and knees, as well as parts that mainly move in the body such as each joint, or parts that serve as a reference (center) for movement.

[0031]

5 The phrase "body part trajectory information" indicates information obtained by forming location information, which is acquired at each predetermined timings such as every 0.1 to 1.0 seconds, into a trajectory as a continuous change in location in a real space.

[0032]

10 The phrase "movement of the body" includes not only movements of each part or complex parts such as rotating (including various rotating methods), raising, or lowering arms (both or either of left and right), waving palms (both or either of left and right), shaking (front and back, left and right) or rotating the head, raising (various raising methods) or lowering a leg (either left or right), or moving or bending the upper
15 body, but also whole-body movements such as walking, jumping, or changing a posture (crouching, rising, lying down, etc.).

[0033]

(6) The embodiment of the present invention has a configuration of a terminal device that uses a unique authentication code in which identification information of a
20 user in a virtual space is associated with entity information indicating that the user actually exists in a real space, the terminal device including:

a receiving unit that receives identification information of the user in the virtual space as virtual identification information;

an identification unit that identifies a current location and identifies a time at
25 which the current location is identified;

a request unit that requests a server system to issue a non-fungible authentication code for identity verification for using a given network service by

associating the received virtual identification information with current location information indicating the identified current location and time information indicating the time at which the current location is identified as the entity information; and

5 a service-related process execution unit that executes a service-related process using the authentication code issued based on the issuance request and registered in a given database after being assigned to the user.

[0034]

Based on this configuration, an embodiment of the present invention can associate identification information (i.e., ID) in virtual space with information for
10 proving an entity in real space via the authentication code. Accordingly, even for user activities in the virtual space, the actual existence can be ensured by using the authentication code.

[0035]

In other words, the embodiment of the present invention can allow the user to
15 receive network services by using the authentication code for which reliability for identity authentication is ensured while ensuring anonymity, and therefore can realize various activities such as economic activities of the user in the virtual space comparable to the real space.

[0036]

20 (7) The embodiment of the present invention has a configuration of the terminal device further including a determination unit that executes an expiration date determination process that determines whether an expiration date of the authentication code is exceeded,
wherein the request unit requests the server system to issue the authentication code
25 based on re-acquired current location information and time information in a case where it is determined as a result of the expiration date determination process that the expiration date of the authentication code has passed.

[0037]

Based on this configuration, the embodiment of the present invention can prove legitimacy of the user for each predetermined period by providing an expiration date, and therefore can accurately prevent unauthorized use such as leakage of information or spoofing.

[0038]

(8) The embodiment of the present invention has a configuration of the terminal device, wherein the service-related process execution unit executes the service-related process related to the network service using the authentication code that is encrypted and registered in multiple databases on a network in a distributed manner as a given database.

[0039]

Based on this configuration, the embodiment of the present invention can register the authentication code in a plurality of the databases by using a distributed ledger technology such as a blockchain which is difficult to be falsified, and therefore can improve the reliability of identity authentication.

[0040]

(9) The embodiment of the present invention has a configuration of an authentication code utilization method that uses a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user actually exists in a real space, the authentication code utilization method including:

receiving identification information of the user in the virtual space as virtual identification information;

identifying a current location and identifying a time at which the current location is identified;

requesting a server system to issue a non-fungible authentication code for identity verification for using a given network service by associating the received virtual identification information with current location information indicating the identified current location and time information indicating the time at which the current location is
5 identified as the entity information; and

executing the service-related process related to the network service using the authentication code issued based on the issuance request and registered in a given database after being assigned to the user.

[0041]

10 Based on this configuration, an embodiment of the present invention can associate identification information (i.e., ID) in virtual space with information for proving an entity in real space via the authentication code. Accordingly, even for user activities in the virtual space, the actual existence can be ensured by using the authentication code.

15 [0042]

In other words, the embodiment of the present invention can allow the user to receive network services by using the authentication code for which reliability for identity authentication is ensured while ensuring anonymity, and therefore can realize various activities such as economic activities of the user in the virtual space comparable
20 to the real space.

[0043]

In particular, the embodiment of the present invention can perform identity authentication without identity proofing information being known by others, including an authentication code issuance system, in a case where the identity proofing
25 information is registered so as not to be accessible by anyone other than the user, and therefore can ensure anonymity thereof.

[0044]

(10) The embodiment of the present invention has a configuration of an authentication code issuance method that issues a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user actually exists in a real space, the authentication
5 code issuance method including:

acquiring identification information of the user in the virtual space as virtual identification information;

acquiring, from a terminal device held by the user, current location information indicating a current location of the terminal device and time information indicating a
10 time at which the current location is identified;

issuing a non-fungible authentication code for identity verification for using a given network service, the authentication code being a code of the user's unique identification information, by associating the acquired virtual identification information with the acquired current location information and time information as the entity
15 information; and

registering the issued authentication code in a given database after assigning the issued authentication code to the user.

[0045]

Based on this configuration, an embodiment of the present invention can
20 associate identification information (i.e., ID) in virtual space with information for proving an entity in real space via the authentication code. Accordingly, even for user activities in the virtual space, the actual existence can be ensured by using the authentication code.

[0046]

25 Specifically, the embodiment of the present invention can issue the authentication code for which the reliability of identity authentication is ensured while maintaining anonymity. Accordingly, it is possible to realize various activities such as

economic activities of the user in the virtual space using network services, while ensuring both anonymity and high reliability for identity authentication.

[0047]

Hereinafter, embodiments of the present invention will be described with reference to the drawings.

[0048]

An embodiment described below is an embodiment in which the authentication code issuance system or the terminal device of the present application is applied to a network-based identity authentication system including a token issuance server that issues a Soul Bound Token (SBT) as a non-transferable token (authentication code) on the premise that the user is identity-proofed by an identity proofing provider and location information is acquired, and a terminal device that performs a given transaction using the SBT.

[0049]

Furthermore, the explanation in the present embodiment is given using a Soul Bound Token (SBT) as a digital code for performing identity authentication. However, the digital code is not limited to the SBT, and a unique non-transferable authentication code for which identity authentication has been performed, such as a Non-Fungible Token (NFT), may also be used.

[0050]

[1] Outline of Network-Based Identity Authentication System

First, the outline and system configuration of a network-based identity authentication system S in the present embodiment will be described with reference to Fig. 1.

[0051]

Fig. 1 is a system configuration diagram illustrating the network-based identity authentication system according to the present embodiment.

[0052]

In order to prevent the drawings from becoming complicated, only some terminal devices 20 used by users are shown in Fig. 1. In other words, the network-based identity authentication system S has more terminal devices 20 than shown in Fig.

5 1.

[0053]

(Outline of the System)

As shown in Fig. 1, the network-based identity authentication system S of the present embodiment is a system that issues a Soul Bound Token (SBT) as a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user actually exists in a real space, and is capable of appropriately allowing the user to receive various network services including identity authentication using the issued SBT.

[0054]

15 In particular, the network-based identity authentication system S has a configuration capable of ensuring actual existence by using the authentication code, even for user activities in the virtual space by associating identification information (i.e., ID) in the virtual space with information for proving an entity in the real space (specifically, current location information and time information at which the current location is identified) via the Soul Bound Token (SBT).

[0055]

(System Configuration)

As shown in Fig. 1, the network-based identity authentication system S of the present embodiment includes: a token issuance server 10 that issues the SBT; a terminal device 20 (e.g., terminal devices 20A, 20B, and 20C) connected to the token issuance server 10 via a network such as the Internet and identifying a current location based on satellite signals transmitted from GPS satellites 70; an identity proofing server 30

25

managed by an identity proofing provider and used when the identity is proofed;
multiple databases 40 in which the SBT of each user is registered using blockchain
technology; and a service management server 50 that executes various processes for
managing a given network service.

5 [0056]

The token issuance server 10 is an information processing device that executes
various processes regarding the issuance of SBT by using, for example, an API
(application programming interface) or a predetermined platform.

[0057]

10 In particular, the token issuance server 10, in cooperation with the terminal
device 20, issues a non-fungible authentication code (i.e., SBT) for identity verification
for using a given network service, the authentication code being a code of the user's
unique identification information, by associating identification information of each user
in the virtual space (specifically, an ID for the virtual space) with current location
15 information indicating a current location of the terminal device 20 transmitted from the
terminal device 20 and time information indicating a time at which the current location
is identified.

[0058]

The token issuance server 10 may be configured by one device (or processor)
20 or a plurality of devices (or processors).

[0059]

The user terminal device 20 is a communication terminal device that serves as
an information processing device used by users such as a PC (personal computer), a
tablet-type information communication terminal device, a smart phone, a mobile phone
25 and an HMD.

[0060]

The terminal device 20 is a device connectable to the token issuance server 10 via a network such as the Internet (WAN) or a LAN, and has a configuration for establishing a communication line with the token issuance server 10 by wire or wireless to transmit and receive various data.

5 [0061]

Furthermore, the terminal device 20 has a configuration provided with functions including:

a communication control function for performing communication with the token issuance server 10, such as input information input by a user;

10 a function for acquiring a current location (i.e., current location information) of the terminal device 20;

a function for executing a process regarding identity proofing (hereinafter referred to as "identity proofing process") in cooperation with the identity proofing server 30;

15 a function for registering identity proofing information in the database 40; and

a function for allowing the user to receive a service with the service management server 50 or another terminal device 20 or to execute a given transaction, by using the SBT transmitted from the token issuance server 10.

[0062]

20 In particular, the terminal device 20 has a configuration for acquiring current location information of the terminal device 20 in cooperation with a system for performing high-precision positioning using communication with GPS satellites 70 of a GNSS (Global Navigation Satellite System) including a GPS (Global Positioning System), communication with a base station BS for mobile phones, or short-range
25 wireless communication with a wireless router such as Wi-Fi.

[0063]

The identity proofing server 30 has a configuration that executes an identity proofing process of performing identity proofing of a user based on identity proofing information provided by the terminal device 20, and provides identity-proofed information to the terminal device 20 of the corresponding user or the token issuance server 10 in a case where the identity proofing is successful.

[0064]

The database 40 may be configured by various databases (storage devices and memories in a broad sense) such as a hard disk drive connectable to the network N, or may be added in an information processing device connected to the network N such as a PC (personal computer) or a server.

[0065]

The service management server 50 is an information processing device that executes various processes regarding various network services or electronic commerce, or manages network services or electronic commerce, by using, for example, an API (application programming interface) or a predetermined platform.

[0066]

The service management server 50 may be configured by one device (or processor) or a plurality of devices (or processors).

[0067]

[2] Token Issuance Server

Next, the configuration according to the token issuance server 10 of the present embodiment will be described with reference to Fig. 2.

[0068]

Fig. 2 is one example of a diagram illustrating functional blocks of the token issuance server 10 of the present embodiment.

[0069]

As illustrated in Fig. 2, the token issuance server 10 of the present embodiment includes a processing unit 100, a storage unit 170, an information storage medium 180, and a communication unit 196.

[0070]

5 The token issuance server 10 of the present embodiment may be configured by omitting one or more composing elements illustrated in Fig. 2.

[0071]

The storage unit 170 serves as a work area for the processing unit 100, and the like, and its functions are configured by a RAM (VRAM) or the like.

10 [0072]

Specifically, the storage unit 170 includes a main storage unit 171 used as a work area used when various processes are executed, and an SBT-related information storage unit 172 storing information regarding the issued SBT.

[0073]

15 In particular, the SBT-related information storage unit 172 stores information regarding the issued SBT (including history information) in association with a user ID of each user.

[0074]

20 The storage unit 170 of the present embodiment may be configured such that a part of the configuration having the main storage unit 171 and the user information storage unit 172 is omitted.

[0075]

25 The information storage medium 180 is readable by a computer, and programs, data, and the like are stored in the information storage medium 180. In other words, the information storage medium 180 stores programs for causing the computer to function as the respective units of the present embodiment (programs for causing the computer to execute the processing of the respective units).

[0076]

The processing unit 100 can perform the various processes of the present embodiment based on data read out from programs (data) stored in the information storage medium 180.

5 [0077]

For example, the information storage medium 180 is an optical disk (CD, DVD), a magneto-optical disk (MO), a magnetic disk, a hard disk, a flash memory such as a solid state drive, a magnetic tape, a memory (ROM), or a memory card.

[0078]

10 The communication unit 196 performs various controls to communicate with an external device (for example, the terminal device 20). The functions of the communication unit 196 is configured by hardware of various processors or ASICs for communication, program and so on.

[0079]

15 The processing unit 100 performs the various processes of the present embodiment based on programs (data) stored in the information storage medium 170.

[0080]

The processing unit 100 of the present embodiment may read out the program and data stored in the information storage medium 180, temporarily store the read-out
20 program and data in the storage unit 170, and perform processing based on the program and data.

[0081]

The processing unit 100 executes various processes using the main storage unit 171 in the storage unit 170 as a work area. The processing unit 100 is implemented by
25 hardware such as various processors (CPU, DSP, etc.), and programs.

[0082]

Specifically, the processing unit 100 includes a communication control unit 101, a data management unit 102, a token issuance management unit 103, a token registration management unit 104, a timer management unit 110, and an information providing unit 111.

5 [0083]

The communication control unit 101 establishes communication lines with the terminal device 20 and the like through the network and performs communication with each other.

[0084]

10 The data management unit 102, in cooperation with the communication control unit 101, acquires identification information of a user in the virtual space (hereinafter referred to as "virtual identification information"), current location information, and identity-proofed information transmitted from each terminal device 20 via the communication unit 196.

15 [0085]

The token issuance management unit 103 issues, for each user, an SBT as an authentication code for identity verification based on identification information of the user in the virtual space, location information indicating a location of the user in the real space, and time information indicating a time at which the location is identified.

20 [0086]

The token registration management unit 104 registers the SBT as an authentication code issued by the token issuance management unit 103 in each database 40 in a distributed manner after assigning the SBT to the user.

[0087]

25 The timer management unit 110 has a function of performing measurement from the current date and time or a predetermined timing, and outputs the current time or a measurement result when the predetermined timing is detected.

[0088]

The information providing unit 111 provides, to the corresponding terminal device 20, information to the effect that the SBT has been issued and registered in the database 40 (an access location of the SBT) and information on an access location for
5 accessing the registered SBT.

[0089]

[3] Terminal Device

Next, the configuration of the terminal device 20 of the present embodiment will be described with reference to Fig. 3. Fig. 3 is a functional block diagram
10 illustrating an example of a configuration of the terminal device 20 according to the embodiment.

[0090]

As shown in Fig. 3, the terminal device 20 of the present embodiment includes:
a processing unit 200; a current location detection unit 250; an operation input unit 260
15 configured with a touch panel or the like; a storage unit 270; an information storage medium 280; a display unit 290 configured with display elements such as a liquid crystal panel; a communication unit 296; and a sound output unit 292.

[0091]

The current location detection unit 250 generates location information
20 indicating the current location while detecting the current location of the terminal device 20 at each predetermined timing.

[0092]

For example, the current location detection unit 250 detects a satellite signal (GPS signal) transmitted from GPS satellites (not shown) while recognizing the location
25 of the GPS satellites at each predetermined period (for example, every 5 seconds).

[0093]

The current location detection unit 250 calculates (i.e., detects) coordinate values of a current location (for example, latitude and longitude) of its terminal device 20 based on the detected GPS signal, and provides the coordinate values as current location information to the processing unit 200.

5 [0094]

The current location detection unit 250 may detect coordinates of a current location or execute correction of the coordinates using Wi-Fi or radio waves for mobile phones instead of or in addition to GPS signals.

[0095]

10 The operation input unit 260 is a device for inputting input information from a user, and outputs the user's input information to the processing unit 200.

[0096]

The operation input unit 260 of the present embodiment includes a detection unit 262 that detects input information (input signal) of a user, and is configured with, for example, a lever, a button, a microphone, a touch panel display, a keyboard, a mouse, or the like.

15 [0097]

The storage unit 270 serves as a work area for the processing unit 200, and the like, and its functions are configured by a RAM (VRAM) or the like.

20 [0098]

The storage unit 270 of the present embodiment includes a main storage unit 271 used as a work area, an image buffer 272 storing a final display image, and a user information storage unit 273 storing user information. Note that one or more of these units may be omitted from the configuration.

25 [0099]

The information storage medium 280 is computer-readable, and stores, in addition to various applications and an OS (operating system), various types of data

including a user ID of a user corresponding to the terminal device 20 particularly in the present embodiment.

[0100]

5 In other words, the information storage medium 280 stores applications for causing a computer to function as the respective units of the present embodiment (applications for causing the computer to execute the process of the respective units) and a user ID.

[0101]

10 For example, the information storage medium 280 is an optical disk (CD, DVD), a magneto-optical disk (MO), a magnetic disk, a hard disk drive, a flash memory, a magnetic tape, a memory (ROM), a memory card, or the like.

[0102]

15 The communication unit 296 performs various types of control for communicating with an external part (for example, another terminal device 20, the token issuance server 10, the identity proofing server 30, the database 40, or the service management server 50), and its functions are configured with hardware such as various processors or a communication ASIC, a program, or the like.

[0103]

20 The processing unit 200 can perform various processes of the present embodiment by reading out and executing the applications stored in the information storage medium 280. The types of applications stored in the information storage medium 280 are arbitrary.

[0104]

25 The processing unit 200 performs various processes of the present embodiment based on the applications stored in the information storage medium 280. The processing unit 200 of the present embodiment may read out the program and data stored in the

information storage medium 280, temporarily store the read-out program and data in the storage unit 270, and perform processing based on the program and data.

[0105]

5 The processing unit 200 executes various processes using the main storage unit 271 in the storage unit 270 as a work area. The processing unit 200 is implemented by hardware such as various processors (CPU, DSP, etc.), and programs.

[0106]

10 The processing unit 200 includes: a communication control unit 210; a Web browser 211; a current location management unit 212; a display control unit 213; an input receiving processing unit 214; an identity proofing processing unit 216; a wallet management unit 217; a timer management unit 218; a drawing unit 220; and a sound processing unit 230. Note that one or more of these units may be omitted from the configuration.

[0107]

15 The communication control unit 210 performs a process of transmitting and receiving data with the token issuance server 10, the identity proofing server 30, the database 40, or the service management server 50.

[0108]

20 The communication control unit 210 receives data transmitted from the token issuance server 10, the identity proofing server 30, the database 40, or the service management server 50, and performs a process of storing the received data in the storage unit 270, a process of providing or registering given data, and a control process or the like related to transmission and reception of other data.

[0109]

25 The communication control unit 210 may perform a process of storing and managing destination information (IP address, port number) of the token issuance server

10, the identity proofing server 30, the database 40, or the service management server 50 in the information storage medium 280.

[0110]

5 The Web browser 211 is an application program for browsing Web pages (an authentication screen, an identity proofing process screen, an identity information registration screen, or a service enjoyment screen), downloads HTML files, image files, or the like from a Web server (the token issuance server 10, the identity proofing server 30, or the service management server 50), analyzes layouts, and controls display.

[0111]

10 The Web browser 211 transmits data to a Web server (the token issuance server 10, the identity proofing server 30, or the service management server 50) using an input form (a link, a button, a text box, or the like).

[0112]

15 The terminal device 20 can display information from a Web server (the token issuance server 10, the identity proofing server 30, or the service management server 50) specified by a URL via the Internet using the Web browser 211.

[0113]

20 For example, the terminal device 20 can display each content (data such as HTML) received from the token issuance server 10, the identity proofing server 30, or the service management server 50 using the Web browser 211.

[0114]

25 The current location management unit 212 acquires current location information at each predetermined period acquired from the current location detection unit 250, and stores the current location information in the main storage unit 271 as history information.

[0115]

The current location management unit 212 transmits the user's current location information to the token issuance server 10 at the time of a request for issuance of an SBT.

[0116]

5 The display control unit 213 performs a process of displaying on the display unit 290. For example, the display control unit 213 may perform display using the Web browser 211.

[0117]

10 The input receiving processing unit 214 recognizes input information input by a user via the operation input unit 260, and executes various processes based on the recognized information.

[0118]

15 The identity proofing processing unit 216 operates in conjunction with the identity proofing server 30 to execute various processes for performing identity proofing of the user based on the identity proofing information, which includes information of identification documents such as a passport, a health insurance card, or a driver's license, or information of identification documents issued by a public organization such as certificates issued by a public organization.

[0119]

20 The wallet management unit 217 operates in conjunction with another terminal device 20 or the service management server 50 to execute various network services or various processes related to electronic commerce.

[0120]

25 In particular, the wallet management unit 217 has access authority to the stored data of the user's SBT in a case where the user's SBT is issued and recorded on a blockchain (in other words, in a case where the user's SBT is encrypted and registered in the database 40 in a distributed manner).

[0121]

The wallet management unit 217 has a unique wallet address and performs signing and verification of a transaction using the wallet address and the SBT.

[0122]

- 5 The wallet management unit 217 generates a private key and a public key (which may be a wallet address) of a user, and executes signing and verification of a transaction using these keys.

[0123]

- 10 For example, the wallet management unit 217 encrypts a private key of a user, stores the encrypted private key in a plurality of databases 40 (in other words, distributed storage), is accessed through a given authentication process by the user, and executes signing and verification of a transaction related to data and an action of the user.

[0124]

- 15 The timer management unit 218 has a function of performing measurement from the current date and time or a predetermined timing, and outputs the current time or a measurement result when the predetermined timing is detected.

[0125]

- 20 The drawing unit 220 performs a drawing process based on various processes performed by the processing unit 200, thereby generates an image, and outputs the image to the display unit 290 using the display control unit 213.

[0126]

- 25 The sound controller 230 executes the sound process based on the results of various processes performed by the processor 200, generates a BGM, an effect sound, a voice or the like, and outputs the sound to the sound output unit 292.

[0127]

[4] Method of the Present Embodiment

[4.1] Outline

Next, an authentication code issuance process executed by the token issuance server 10 and an authentication code issuance request process executed by the terminal device 20 according to the present embodiment will be described with reference to Fig.

5 4.

[0128]

Fig. 4 is a diagram for explaining an authentication code issuance process executed in the token issuance server 10 and an authentication code issuance request process executed by the terminal device 20 according to the present embodiment.

10 [0129]

(Authentication Code Issuance Process)

The token issuance server 10 according to the present embodiment has a configuration to issue an SBT as a unique authentication code in which an owner of the authentication code cannot be changed to another owner and in which identification information of a user in a virtual space (such as a nickname, a handle name, or a pen name) is associated with entity information indicating that the user exists in a real space.

15 [0130]

In particular, the token issuance server 10 according to the present embodiment has a configuration capable of performing accurate identity verification and ensuring actual existence of even user activities in the virtual space, including economic activities, by associating the identification information (in other words, ID) in the virtual space with information for proving the entity in the real space via the SBT.

20 [0131]

Specifically, as shown in Fig. 4, the token issuance server 10 has a configuration to execute:

25

(A1) a virtual identification information acquisition process of acquiring the identification information of the user in the virtual space as the virtual identification information;

5 (A2) a current location information acquisition process of acquiring, from the terminal device 20 held by the user, the current location information indicating the current location of the terminal device 20 and the time information indicating the time at which the current location is identified;

(A3) an SBT issuance process of issuing the SBT as a non-fungible authentication code for the identity verification to be used for a given network service, the SBT being a code
10 of the user-unique identification information, by associating the acquired virtual identification information with the acquired current location information and the acquired time information as the entity information; and

(A4) an SBT registration process of registering the issued SBT as the authentication code in the databases 40 after assigning the issued SBT to the user.

15 [0132]

Note that Fig. 4 shows, in addition to each of the processes described above, transmission to the effect that the SBT is issued and registered in the databases 40 (the access location of the SBT) in a case where the SBT is issued by the token issuance server 10, and verification using the SBT and the wallet address in a case where a
20 transaction such as a commercial transaction or a settlement is executed using the SBT.

[0133]

By having such a configuration, the token issuance server 10 according to the present embodiment can issue the authentication code for which reliability for the identity verification is ensured while ensuring anonymity. Accordingly, it is possible to
25 realize various activities such as the economic activities of the user in the virtual space using the network service, while ensuring both the anonymity and the high reliability for the identity verification.

[0134]

In particular, the token issuance server 10 according to the present embodiment can realize highly reliable and highly immediate identity verification and transaction verification based on the result thereof while ensuring the anonymity of the user, in a situation where decentralized management of data and information by individuals is increasing, such as in the decentralized internet (Web 3.0) or Dapps (Decentralized Applications), and individual activities are becoming active even in the virtual space.

[0135]

In the present embodiment, while identification information having anonymity such as the nickname different from a real name is used as the identification information of the user, it goes without saying that a real name such as the name of the user may be used as the identification information of the user. Note that in this case, although the effect is diminished from the viewpoint of ensuring anonymity, it is possible to improve the reliability for the identity verification and to improve the security against the use of the network service such as spoofing.

[0136]

(Authentication Code Issuance Request Process)

The terminal device 20 according to the present embodiment has a configuration to request the issuance of the SBT and to use the issued SBT in order to prove the authenticity of the user without performing various identity verifications when using the given network service.

[0137]

Specifically, the terminal device 20 according to the present embodiment has a configuration to use the SBT as the unique authentication code in which the identification information of the user in the virtual space is associated with the entity information indicating that the user exists in the real space.

[0138]

In particular, the terminal device 20 according to the present embodiment has a configuration capable of performing the accurate identity verification and ensuring the actual existence of even the user activities in the virtual space, including the economic activities, by requesting the issuance of the SBT and using the SBT, in which the
5 identification information (in other words, ID) in the virtual space is associated with the information for proving the entity in the real space.

[0139]

Specifically, the terminal device 20 has a configuration to execute:

- (B1) a virtual identification information receiving process of receiving the identification
10 information of the user in the virtual space as the virtual identification information;
- (B2) a current location identification process of identifying the current location and identifying the time at which the current location is identified;
- (B3) an SBT issuance request process of requesting the server system to issue the SBT as the non-fungible authentication code for the identity verification in order to use the
15 given network service, by associating the received identification information with the current location information indicating the identified current location and the time information indicating the time at which the current location is identified as the entity information; and
- (B4) a service-related process of executing a process related to the network service
20 using the SBT that is issued based on the issuance request for the SBT and registered in the databases 40 after being assigned to the user.

[0140]

Note that Fig. 4 shows, in addition to each of the processes described above, a request for an identity proofing process to the identity proofing server 30, provision of
25 identity proof information, and execution of the identity proofing process in the identity proofing server 30.

[0141]

By having such a configuration, the token issuance server 10 according to the present embodiment can receive the network service by using the authentication code for which the reliability for the identity verification is ensured while ensuring the anonymity, thereby making it possible to realize various activities such as the economic activities of the user in the virtual space comparably to those in the real space.

[0142]

[4.2] Identity-Proofed Information Acquisition Process (a Preliminary Process for the Authentication Code Issuance Process)

Next, the identity-proofed information acquisition process as the preliminary process for the authentication code issuance process executed by the token issuance server 10 according to the present embodiment will be described.

[0143]

In a case where receiving the authentication code issuance request transmitted from the terminal device 20, as shown in Fig. 4, the data management unit 102 executes the identity-proofed information acquisition process of acquiring the identity-proofed information indicating that the user has been identity-proofed by the identity proofing provider based on the unique identity proof information, the identity-proofed information being transmitted from the terminal device 20 together with the authentication code issuance request.

[0144]

In particular, the data management unit 102 performs the identity proofing based on the identity proofing information such as information on identification documents issued by a public organization (for example, a passport, an insurance card, or a driver's license) or information on certificates issued by a public institution (for example, a certificate of residence) in cooperation with the identity proofing server 30 via the terminal device 20 of the corresponding user, and determines whether or not the

identity-proofed information indicating that the identity proofing is successful is acquired.

[0145]

5 When acquiring the identity-proofed information indicating that the identity proofing is successful, the data management unit 102 executes the authentication code issuance process. Further when the identity-proofed information cannot be acquired, the data management unit 102 stops the issuance of the SBT based on the authentication code issuance request.

[0146]

10 For example, the identity proofing provider is the highly reliable provider that is the government or that is requested or permitted by the government and is constrained by the public and the legal requirements.

[0147]

[4.3] Virtual Identification Information Receiving Process and Current Location

15 Information Acquisition Process

Next, the virtual identification information acquisition process and the current location information acquisition process of the authentication code issuance process executed by the token issuance server 10 according to the present embodiment will be described.

20 [0148]

(Virtual Identification Information Acquisition Process)

When receiving the authentication code issuance request transmitted from the terminal device 20, as shown in Fig. 4, the data management unit 102 executes the virtual identification information acquisition process of acquiring the identification
25 information of the user in the virtual space transmitted from the terminal device 20 via the communication unit 196 as the virtual identification information in cooperation with the communication control unit 101.

[0149]

In particular, when receiving the authentication code issuance request transmitted from the terminal device 20, the data management unit 102 acquires the identification information of the user in the virtual space transmitted from the terminal device 20, such as the nickname, the handle name, or the pen name, as the virtual identification information, in order to ensure the anonymity of the user.

[0150]

Note that the virtual identification information may be the information identified by the wish of each user, or may be automatically assigned, but the virtual identification information is the unique information and is preferably assigned to be distinguished from the virtual identification information of the other users.

[0151]

(Current Location Information Acquisition Process)

When receiving the authentication code issuance request transmitted from the terminal device 20, as shown in Fig. 4, the data management unit 102 executes, similarly to the virtual identification information, the current location information acquisition process of acquiring the current location information transmitted from the terminal device 20 via the communication unit 196 in cooperation with the communication control unit 101.

[0152]

In particular, when receiving the authentication code issuance request transmitted from the terminal device 20, the data management unit 102 executes the current location information acquisition process of acquiring the current location information indicating the current location of the terminal device 20 and the time information indicating the time at which the current location is identified, the current location information and the time information being transmitted from the terminal device 20.

[0153]

Specifically, the data management unit 102 acquires, from the terminal device 20 that transmits the authentication code issuance request, the current location information of the terminal device 20 (namely, the user's current location information) and the time information indicating the time at which the current location is identified, in order to prove that the user exists and issue the SBT by using the current location information and the time information as the biological information of the user.

[0154]

[4.4] SBT Issuance Process and SBT Registration Process (Authentication Code Issuance Process)

Next, the SBT issuance process and the SBT registration process of the authentication code issuance process executed by the token issuance server 10 according to the present embodiment will be described.

[0155]

(SBT Issuance Process)

When acquiring the virtual identification information, the current location information, and the time information by the virtual identification information acquisition process and the current location information acquisition process together with the authentication code issuance request, the token issuance management unit 103 executes, as shown in Fig. 4, the SBT issuance process of issuing the SBT as the non-fungible authentication code for the identity verification for using the given network service, the SBT being the code of the user-specific identification information, by associating the acquired virtual identification information with the acquired current location information and the acquired time information as the entity information.

[0156]

In particular, at this time, the token issuance management unit 103 acquires the wallet address from the corresponding terminal device 20.

[0157]

The token issuance management unit 103 issues the SBT (Soul Bound Token) as the non-transferable NFT (Non-Fungible Token: the digital data with the non-forgeable certificate of authenticity and the ownership certificate) which is always
5 linked to the individual wallet address and cannot be sold or transferred to the other person.

[0158]

The token issuance management unit 103 issues the SBT having the predetermined expiration date such as the one day or the one week in order to verify the
10 entity of the user at each of the predetermined timings.

[0159]

Note that in the present embodiment, on the premise of acquiring the identity-proofed information as the Verifiable Credentials (hereinafter referred to as the "verifiable credentials") (namely, that the identity proofing is executed), the token
15 issuance management unit 103 issues the SBT as the unique authentication code non-transferable to the other users based on the virtual identification information, the current location information, and the time information.

[0160]

(SBT Registration Process)

20 When issuing the SBT as the authentication code by the token issuance management unit 103, as shown in Fig. 4, the token registration management unit 104 registers the issued SBT in the plurality of databases 40 in a distributed manner after assigning the issued SBT to the user.

[0161]

25 In particular, the token registration management unit 104 encrypts the issued SBT and registers the encrypted SBT in the plurality of databases 40 on the network in a distributed manner using, for example, blockchain technology.

[0162]

At this time, the token registration management unit 104 registers the SBT in the plurality of databases 40 in a distributed manner so as to be non-transferable to the other person while being usable on the network, by associating the SBT with the wallet address assigned to the wallet application of the corresponding user.

[0163]

When registering the SBT, the token registration management unit 104 provides, via the information providing unit 111, the effect that the SBT is registered together with the access position information for accessing the registered SBT to the corresponding terminal device 20.

[0164]

Note that in the present embodiment, although the SBT, which is the non-transferable token, is issued as the authentication code, the digital code such as the electronic certificate may be used when the digital code is non-transferable.

[0165]

Further, in the present embodiment, the token registration management unit 104 registers the SBT as the authentication code in the plurality of databases 40 in a distributed manner using blockchain technology, after associating the SBT with the wallet address and assigning the SBT to the user. However, the token registration management unit 104 having the uniqueness of the terminal device 20 for using the given network service, such as the virtual identification information, the ID (the UID) of the terminal device 20, or the number (the so-called mobile phone number) in the case where the terminal device 20 has the function of the mobile phone, may be used instead of the wallet address.

[0166]

[4.5] Identity Proofing Process (Preliminary Process of Authentication Code Issuance Request Process)

Next, the identity proofing process as the prerequisite process of the authentication code issuance request process executed by the terminal device 20 will be described.

[0167]

5 When transmitting the authentication code issuance request, the identity proofing processing unit 216 executes, as shown in Fig. 4, the identity proofing request process of requesting the identity proofing based on the identity proof information showing the identity of the user in cooperation with the identity proofing server 30.

[0168]

10 In particular, the identity proofing processing unit 216 provides the information such as the name, the address, the phone number, or the credit card number as the identity proofing information, and requests the identity proofing to the identity proofing server 30 based on the identity proof information such as the identification document issued by the public organization including the passport, the insurance card, or the
15 driver's license, or the information of the certificate issued by the public organization such as the residence certificate.

[0169]

 The identity proofing server 30 may automatically execute the identity proofing process by using the provided identity proofing information, the identity proof
20 information, and the like, or may execute the identity proofing process by using the human resources.

[0170]

 When receiving the effect that the identity proofing process is successful in the case where the identity proofing process is executed by the identity proofing server 30,
25 the identity proofing processing unit 216 registers the information showing the identity proofing (namely, the identity-proofed information) in the user information storage unit 273 as being identity-proofed.

[0171]

When receiving the effect that the identity proofing process fails from the identity proofing server 30, the identity proofing processing unit 216 causes the display unit 290 to display the notification to that effect in cooperation with the display control unit 213.

[0172]

At this time, the identity proofing processing unit 216 may execute the identity proofing request process again or may forcibly terminate the identity proofing request process.

[0173]

[4.6] Virtual Identification Information Receiving Process and Current Position Identification Process (Authentication Code Issuance Request Process)

Next, the virtual identification information receiving process and the current position specification process of the authentication code issuance request process executed by the terminal device 20 will be described.

[0174]

(Virtual Identification Information Receiving Process)

When transmitting the authentication code issuance request, the input receiving processing unit 214 receives, as shown in Fig. 4, the identification information of the user in the virtual space as the virtual identification information based on, for example, the operation to the operation input unit 260 by the user.

[0175]

For example, the input receiving processing unit 214 receives the identification information for distinguishing from the other user in the virtual space, such as the nickname, the handle name, or the pen name, as the virtual identification information.

[0176]

(Current Position Specification Process)

When transmitting the authentication code issuance request, the current position management unit 212 identifies, as shown in Fig. 4, the current position of the terminal device 20 as the current position identification process, while identifying the time when the current position is identified, based on the GPS signal received by the current position detection unit 250.

[0177]

In particular, the current position management unit 212 may use the location information identified using the GPS signal, or may execute the coordinates of the current position or the correction thereof by using the Wi-Fi or the radio wave for the mobile phone instead of or in addition to the GPS signal.

[0178]

[4.7] SBT Issuance Request Process (Authentication Code Issuance Request Process),
Wallet Function and Others

Next, the SBT issuance request process, the management and the reissuance of the SBT, and the wallet function using the SBT of the authentication code issuance request process executed by the terminal device 20 will be described.

[0179]

(SBT Issuance Request Process)

When transmitting the authentication code issuance request and acquiring the virtual identification information received by the virtual identification information receiving process, the current location information showing the identified current location and the time information showing the time at which the current location is identified as the entity information, the wallet management unit 217 requests, as shown in Fig. 4, the issuance of the SBT as the non-fungible authentication code for the identity verification for using the given network service to the token issuance server 10 by associating the acquired virtual identification information with the acquired current location information and the acquired time information.

[0180]

(SBT Management and Reissuance Request)

The wallet management unit 217 manages the expiration date of the SBT registered in each database 40 in a distributed manner at the predetermined timing.

5 [0181]

In particular, the wallet management unit 217 recognizes the timing of using the function of the wallet or the expiration date determined when the SBT is issued as the predetermined timing, and transmits the request for the reissuance of the SBT at the timing based on the recognized expiration date because the expiration date is stored in the SBT and the SBT becomes unusable after the expiration date.

[0182]

Specifically, the wallet management unit 217 acquires the information of the expiration date from the information of the corresponding SBT based on the wallet address for each database 40 at the predetermined timing, and executes the determination process for determining whether it is within the certain period until the expiration date or whether the expiration date is exceeded.

[0183]

When detecting that it is within the certain period until the expiration date (for example, one day before the expiration date) or that the expiration date is exceeded, the wallet management unit 217 transmits the request for the reissuance of the SBT.

[0184]

(Wallet Function)

The wallet management unit 217 has the wallet address for identifying the wallet from the wallet of the other user as the digital wallet, and manages the application having the function of providing the settlement data to the other terminal device 20 or the service management server 50 by using the wallet address and by using the wireless, the Bluetooth (registered trademark), or the magnetic function.

[0185]

In particular, the wallet management unit 217 has access authority to the stored data of the user's SBT in a case where the user's SBT is issued and recorded on a blockchain (in other words, in a case where the user's SBT is encrypted and registered in the database 40 in a distributed manner).

[0186]

The wallet management unit 217 executes the service-related process related to the network service such as the financial service or the EC site by using the SBT as the authentication code registered in the database 40.

10 [0187]

In other words, the wallet management unit 217 executes the service-related process related to the given network service by using the SBT issued based on the issuance request and registered in the given database after assigning the SBT to the user.

[0188]

15 Specifically, when executing the transaction such as the settlement or the commercial transaction, the wallet management unit 217 provides the information of the SBT together with the wallet address to the settlement destination or the transaction destination to cause the service management server 50 or the other terminal device 20 of the settlement destination or the commercial transaction destination in order to execute the verification of the transaction, as shown in Fig. 4.

[0189]

[5] Operation in the present embodiment

[5.1] Authentication Code Issuance Request Process

25 Next, the operation of the authentication code issuance request process executed by the terminal device 20 of the present embodiment will be described with reference to Figs. 5 and 6.

[0190]

Figs. 5 and 6 are the flowcharts illustrating the operation of the authentication code issuance request process executed by the terminal device 20 of the present embodiment.

[0191]

5 First, when receiving the instruction for the issuance of the authentication code of the user through the operation input unit 260 (step S101), the input receiving processing unit 214 executes the determination process of determining whether the issuance is the issuance of the first authentication code or the issuance of the second and subsequent authentication codes based on the instruction of the user (step S102).

10 [0192]

When determining that it is the issuance of the first authentication code, the input receiving processing unit 214 proceeds to the process of the step S103, and when determining that it is not the issuance of the first authentication code, the input receiving processing unit 214 proceeds to the process of the step S111.

15 [0193]

Next, when being determined by the input receiving processing unit 214 that it is the issuance of the first authentication code, the identity proofing processing unit 216 acquires the identity proofing information while interlocking with the input receiving processing unit 214 and the operation input unit 260 and while prompting the input of the predetermined identity proofing information such as the name, the address, the telephone number, or the credit card number (step S103).

[0194]

In the present embodiment, the information described in the identification document provided in the identity proofing process is required as the identity proofing information.

25

[0195]

Next, the identity proofing processing unit 216 transmits, to the identity proofing server 30, an identity proofing request including the registered identity proofing information and information of an identity proofing document such as a passport, a health insurance card, a driver's license, or a certificate issued by a public organization (step S105).

[0196]

Next, the identity proofing processing unit 216 executes the determination process of determining whether the identity proofing of the user is completed (succeeded) while interlocking with the identity proofing server 30 (step S106).

[0197]

When determining that the identity proofing is not successful (is not able to be completed), the identity proofing processing unit 216 notifies the user that the identity proofing fails (step S107) and proceeds to the process of the step S103. The identity proofing processing unit 216 may forcibly terminate the present operation at the present point based on the operation of the user.

[0198]

Next, when determining that the identity proofing is successful (is able to be completed), the identity proofing processing unit 216 receives the identity-proofed information and registers the received identity-proofed information in the user information storage unit 273 (step S108).

[0199]

The identity-proofed information includes the various types of information such as the information regarding the identity proofing provider being the name of the identity proofing provider that performs the identity proofing, the registered time, or the ID of the user.

[0200]

Next, the input receiving processing unit 214 receives the identification information of the user in the virtual space as the virtual identification information based on the operation of the user to the operation input unit 260 (step S111).

[0201]

5 Next, the current location management unit 212 detects the current location based on the GPS signal and acquires the current time at the timing detected by the timer management unit 218 (step S112).

[0202]

10 Next, the wallet management unit 217 requests the issuance of the SBT as the authentication code to the token issuance server 10 together with the virtual identification information, the current location information (including current time information) indicating the identified current location, and the time information when the current location information is identified (step S113).

[0203]

15 Next, when recognizing that the SBT is issued (step S114), the wallet management unit 217 registers the access location of the SBT on the database 40 in the user information storage unit 273 (step S115) and terminates the present operation.

[0204]

20 Next, when recognizing that the SBT is not issued (step S114), the wallet management unit 217 causes the display unit 290 to display the cancellation of the issuance of the SBT (step S116) and terminates the present operation.

[0205]

25 When requested for the authentication based on the SBT from the other terminal device 20 or the service management server 50, the wallet management unit 217 provides the information of the wallet address and the access location of the SBT. In this case, when the expiration date of the SBT passes, the wallet management unit 217 starts the present operation from the process of the step S101 and provides the

information of the wallet address and the access location of the newly issued SBT after the issuance of the new SBT.

[0206]

[5.2] Authentication Code Issuance Process

5 Next, the operation of the authentication code issuance process executed by the token issuance server 10 of the present embodiment will be described with reference to Fig. 7.

[0207]

10 Fig. 7 is the flowchart showing the operation of the authentication code issuance process executed by the token issuance server 10 of the present embodiment.

[0208]

15 First, when receiving the authentication code issuance request transmitted from the terminal device 20 (step S201), the data management unit 102 acquires the virtual identification information, the current location information, and the time information included in the authentication code issuance request (step S202).

[0209]

20 Next, the token issuance management unit 103 executes the issuance determination process of determining whether or not the SBT is issued based on the virtual identification information, the current location information, and the current time information (step S203).

[0210]

25 For example, the token issuance management unit 103 also: acquires the identity-proofed information; determines that the identity-proofed information is valid information; and determines that the current location is a location in the real space and that the time in the current time information is within a predetermined range based on the current time and the like.

[0211]

At that time, when determining that the SBT is to be issued, the token issuance management unit 103 issues the SBT (step S204), registers the issued SBT in the plurality of databases 40 in a distributed manner, transmits the access location of the database 40 storing the SBT to the corresponding terminal device 20 (step S205), and
5 terminates the present operation.

[0212]

On the other hand, when determining not to issue the SBT, the token issuance management unit 103 interlocks with the information providing unit 111, transmits the effect to the terminal device 20 (step S206), and terminates the present operation.

10 [0213]

[6] Modification

[6.1] Modification 1

Next, modification 1 according to the present embodiment will be described.

[0214]

15 In the present embodiment, while the current location information of the terminal device 20 is used for the presence or the absence of the existence of the user in the real space, the token issuance server 10, for example, registers the activity area for each of the users by the nationality (for example, Japanese) or the address of the user included in the identity proofing information, determines whether or not the detected
20 current location of the terminal device 20 is the pre-registered activity area, and when the detected current location is within the activity area, may issue the SBT.

[0215]

[6.2] Modification 2

Next, modification 2 according to the present embodiment will be described
25 with reference to Figs. 8 to 10.

[0216]

Fig. 8 is the system configuration diagram showing the configuration of the network-type identity authentication system in modification 2 of the present embodiment. Fig. 9 is the diagram for explaining the motion capture process of the user executed in the information processing server in modification 2 of the present
5 embodiment.

[0217]

Fig. 10 is a diagram for explaining a motion capture process of the user executed in the token issuance server in the second modification of an embodiment.

[0218]

10 (System Overview and Configuration)

The present modification is characterized by recognizing the physical movement of the user based on the current location information used when executing the authentication code issuance process, and additionally executing the identity authentication using the recognized movement.

15 [0219]

Specifically, as shown in Fig. 8, similarly to the above, the network-type identity authentication system S of the present modification is configured by the token issuance server 10, the terminal device 20 (for example, terminal devices 20A, 20B, and 20C), the identity proofing server 30, the plurality of the databases 40, and the service
20 management server 50.

[0220]

As shown in Fig. 8, in addition to the above configuration, the network-type identity authentication system S of the present modification has the information processing server 60 that recognizes the physical movement (motion) of the user using
25 the network and executes the motion capture process of outputting the recognized physical movement of the user as the motion information while using the current location information for each of the predetermined periods.

[0221]

In the network-type identity authentication system S of the present modification, the same member as the above embodiment is assigned the same reference numeral, and the description thereof is omitted.

5 [0222]

(Information Processing Server Device)

As shown in Fig. 9, the information processing server 60 of the present modification has the configuration to execute:

- 10 (A1) the process of acquiring the information showing the physical feature of the user P as the physical information (namely, process including process of reading user information and process of identifying and acquiring physical information based on input support using terminal device 20);
- (A2) the process of acquiring the current location information of the terminal device 20 that exists in association with the part of the body of the user P (namely, specific part)
- 15 and moves with the movement of the part (hereinafter referred to as "part location information acquisition process");
- (A3) the process of detecting the trajectory of the part of the body of the user as part trajectory information based on the location information of the terminal device 20 (hereinafter referred to as "part trajectory information detection process");
- 20 (A4) the motion recognition process of recognizing the physical movement of the body of the user based on the acquired physical information and the detected part trajectory information; and
- (A5) the output control process of outputting the recognized physical movement as the motion information to the token issuance server 10.

25 [0223]

Namely, the information processing server 60 has the configuration of realizing the motion capture of digitally acquiring the movement of the user itself or the part of the body of the user (so-called motion) using the current location information.

[0224]

5 (Token Issuance Server Device)

As shown in Fig. 10, the token issuance server 10 of the present modification has the configuration of:

- (B1) managing, as the user information, the user information regarding the user corresponding to each of the stored users, the user information being the motion feature information showing the feature of the movement of the part of the body of the user;
- 10 (B2) identifying the user (hereinafter referred to as "target user") who is the target of the motion information output from the information processing server 60;
- (B3) executing the determination process of determining the identity of the movement of the physical part of the identified user based on the motion feature information
- 15 (namely, reference motion information) of the identified target user and the motion information (namely, recognized motion information) output from the information processing server 60;
- (B4) when determining that the movement of the part shown by the motion feature information and the movement of the physical part of the user shown by the motion
- 20 information are the movement that is the same or is regarded as being the same in the determination process, executing the authentication process of performing the identity authentication of the corresponding user; and
- (B5) issuing the SBT to the user who is identity-authenticated as described above.

[0225]

- 25 The token issuance server 10 has the configuration for executing the identity authentication as the biometric authentication based on the motion information while

using the motion information obtained by the process of the motion capture as the biometric information.

[0226]

[6.3] Modification 3

5 Next, modification 3 of the present embodiment will be described.

[0227]

 In the above embodiment, while the issuance of the SBT is executed on the premise that the identity proofing based on the identification document by the identity proofing server 30 is successful, even when not executing the identity proofing, the SBT
10 may be issued based on the location information of the terminal device 20, the time information, and the identification information in the virtual space.

[0228]

[6.4] Modification 4

 Next, modification 4 of the present embodiment will be described.

15 [0229]

 In the above embodiment, while described using the information terminal device such as the smartphone as the example of the terminal device, the SBT may be provided to the IoT device such as the IoT sensor.

[0230]

20 In this case, since the authenticity of the data generated by the IoT device is capable of being secured, for example, the monitoring of the supply-chain-related data, the improvement of the transparency from the shipment of the product to the end user, and the verification or the analysis of the situation such as the quality, the safety, the reliability, and the human rights protection of the product become possible.

25 [0231]

[7] Others

The embodiment of the present invention is not limited to the one described in the above embodiment, and the various modifications are possible. For example, words cited as broadly or synonymously in the description or drawings may be replaced by broadly or synonymously in the description or drawings.

5 [0232]

The present embodiment includes substantially the same configuration as the configuration described in the embodiment (for example, configuration with the same function, method and result, or configuration with the same purpose and effect). The present invention also includes a configuration in which non-essential parts of the configuration described in the embodiment are replaced. The present invention also includes a configuration that achieves the same effects as the configuration described in the embodiment or a configuration that can achieve the same purpose. The present invention also includes a configuration obtained by adding a known technique to the configuration described in the above embodiment.

15 [0233]

Although the present embodiments of the present invention have been described in detail as described above, it will be readily apparent to those skilled in the art that many variations are possible without departing materially from the new matter and effect of the present invention. Accordingly, all such modifications are intended to be within the scope of the present invention. DESCRIPTION OF REFERENCE SIGNS

[0234]

S: Network-Based Identity Authentication System

10: Token Issuance Server Device

20: Terminal Device

25 30: Identity Proofing Server Device

40: Database

50: Service Management Server

- 60: Information Processing Server
- 70: GPS Satellite
- 100: Processing Unit
- 101: Communication Control Unit
- 5 102: Data Management Unit
- 103: Token Issuance Management Unit
- 110: Timer Management Unit
- 111: Information Providing Unit
- 170: Storage Unit
- 10 171: Main Storage Unit
- 172: SBT-Related Information Storage Unit
- 180: Information Storage Medium
- 196: Communication Unit
- 200: Processing Unit
- 15 210: Communication Control Unit
- 211: Web Browser
- 212: Current Location Management Unit
- 213: Display Control Unit
- 214: Input Receiving Processing Unit
- 20 215: Identity Proofing Information Management Unit
- 216: Identity Proofing Processing Unit
- 217: Wallet Management Unit
- 218: Timer Management Unit
- 220: Drawing Unit
- 25 230: Sound Processing Unit
- 250: Current Location Detection Unit
- 260: Operation Input Unit

262: Detection Unit

270: Storage Unit

271: Main Storage Unit

272: Image Buffer

5 273: User Information Storage Unit

280: Information Storage Medium

290: Display Unit

292: Sound Output Unit

296: Communication Unit

10

CLAIMS

[Claim 1]

An authentication code issuance system for issuing a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the system comprising:

a virtual identification information acquisition unit for acquiring identification information of the user in the virtual space as virtual identification information;

a location information acquisition unit for acquiring, from a terminal device held by the user, current location information indicating a current location of the terminal device and time information indicating a time at which the current location is identified;

an authentication code issuance unit for issuing a non-fungible authentication code for identity verification for using a given network service, the authentication code being a code of identification information unique to the user, by associating the acquired virtual identification information with the acquired current location information and time information as the entity information; and

a registration unit for registering the issued authentication code in a given database after assigning the issued authentication code to the user.

[Claim 2]

The authentication code issuance system according to claim 1, wherein the authentication code issuance unit issues the authentication code having a limited period of use.

[Claim 3]

The authentication code issuance system according to claim 1, wherein

the registration unit encrypts the authentication code and registers the encrypted authentication code in a plurality of the databases on a network in a distributed manner.

5 [Claim 4]

The authentication code issuance system according to claim 1, wherein the authentication code issuance unit issues the authentication code for identity verification by using at least the current location information as biometric information of the user.

10

[Claim 5]

The authentication code issuance system according to claim 4, further comprising

an information management unit for managing user information regarding a user corresponding to each of the users stored in a storage unit, the user information being motion feature information that indicates a feature of movement of a part of a body of the user, wherein

the authentication code issuance unit:
detects a trajectory of the part of the body of the user as part trajectory information based on a plurality of the current location information, and identifies motion information indicating a physical movement of the user based on the detected part trajectory information;

executes a determination process of determining identity of the movement of the physical part of a target user based on the motion feature information of the target user who requested issuance of the authentication code and the identified motion information;

executes an authentication process of performing identity authentication of the target user when it is determined in the determination process that the movement of the part indicated by the motion feature information and the movement of the physical part of the target user indicated by the motion information are
5 movements that are the same or are regarded as being the same; and
issues the authentication code for identity verification when the identity authentication by the authentication process is successful.

[Claim 6]

10 A terminal device utilizing a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the terminal device comprising:

a receiving unit for receiving the identification information of the user in the virtual space as virtual identification information;

15 an identification unit for identifying a current location and a time at which the current location is identified;

a requesting unit for requesting a server system to issue a non-fungible authentication code for identity verification for using a given network service, by associating the received virtual identification information with current location

20 information indicating the identified current location and time information indicating the time at which the current location is identified as the entity information; and

a service-related process execution unit for executing a service-related process associated with the network service using the authentication code that is issued based on an issuance request and registered in a given database after being assigned to the user.

25

[Claim 7]

The terminal device according to claim 6, further comprising

a determination unit for executing a usage expiration determination process for determining whether or not an expiration date of the authentication code is exceeded, wherein

the requesting unit requests the server system to issue the authentication code
5 based on re-acquired current location information and time information when it is determined, as a result of the usage expiration determination process, that the expiration date of the authentication code is exceeded.

[Claim 8]

10 The terminal device according to claim 6, wherein
the service-related process execution unit executes the service-related process associated with the network service using the authentication code that is encrypted and registered in a plurality of databases on a network in a distributed manner as the given database.

15

[Claim 9]

An authentication code utilization method for utilizing a unique authentication code in which identification information of a user in a virtual space is associated with entity information indicating that the user exists in a real space, the method comprising:

20 receiving the identification information of the user in the virtual space as virtual identification information;

identifying a current location and a time at which the current location is identified;

requesting a server system to issue a non-fungible authentication code for
25 identity verification for using a given network service, by associating the received virtual identification information with current location information indicating the

identified current location and time information indicating the time at which the current location is identified as the entity information; and

executing a service-related process associated with the network service using the authentication code that is issued based on an issuance request and registered in a
5 given database after being assigned to the user.

[Claim 10]

An authentication code issuance method for issuing a unique authentication code in which identification information of a user in a virtual space is associated with
10 entity information indicating that the user exists in a real space, the method comprising:

acquiring identification information of the user in the virtual space as virtual identification information;

acquiring, from a terminal device held by the user, current location information indicating a current location of the terminal device and time information indicating a
15 time at which the current location is identified;

issuing a non-fungible authentication code for identity verification for using a given network service, the authentication code being a code of identification information unique to the user, by associating the acquired virtual identification information with the acquired current location information and time information as the
20 entity information; and

registering the issued authentication code in a given database after assigning the issued authentication code to the user.