

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: January 17, 2014

Application Number: JP 2014-006624

The country code and
number of your priority
application, to be used
for filing abroad under
the Paris Convention, is JP2014-006624

Applicant(s): The Ricoh Company, Ltd.

August 20, 2014

Seal of the Commissioner,
Japan Patent Office

Commissioner,
Japan Patent Office

Hitoshi Ito



[Document Name]	Patent Application
[File Number]	201310444
[Submission Date]	January 17, 2014
[Addressee]	Hideo Hato, Commissioner, Japan Patent Office
[International Patent Classification]	H04L12/56
[Inventor]	
[Address or Residence]	c/o The Ricoh Company, Ltd., 1-3-6 Nakamagome, Ota-ku, Tokyo
[Name]	Yoshinaga Kato
[Patent Applicant]	
[Identification Number]	000006747
[Name or Title]	The Ricoh Company, Ltd.
[Agent]	
[Identification Number]	100107766
[Patent Attorney]	
[Name or Title]	Tadashige Ito
[Phone Number]	03-5223-6011
[Contact]	Takao Kato, Patent Attorney 100192636
[Appointed Agent]	
[Identification Number]	100070150
[Patent Attorney]	
[Name or Title]	Tadahiko Ito
[Phone Number]	03-5223-6011
[Priority Claim Based on Previous Application]	
[Filing Number]	JP 2013-134146
[Filing Date]	June 26, 2013
[Indication of Handling Fees]	
[Prepayment Ledger Number]	437147
[Payment Amount]	15,000 yen
[List of Submitted Documents]	
[Document Name]	Specification 1
[Document Name]	Scope of Patent Claims 1
[Document Name]	Abstract 1
[Document Name]	Drawings 1
[General Power of Attorney Number]	1203539
[General Power of Attorney Number]	9911477

[Document Name] Specification

[Title of Invention] COMMUNICATION DEVICE, AND COMMUNICATION SYSTEM AND PROGRAM

[Technical Field]

[0001]

The present invention relates to a communication device, and communication system and program.

[Background Art]

[0002]

In recent years, teleconference systems for conducting remote meetings between distant locations via a communication network, such as the Internet or the like, have become increasingly widespread. Connecting a communication device used in such a teleconferencing system to a communication network using wireless communication, such as wireless LAN or the like, allows for greater flexibility of the installation location compared to wired LAN, and for user convenience to be improved.

[0003]

On the other hand, unlike wired communication, wireless communication has an inherent problem in that data can be surreptitiously observed when the radio waves are intercepted. In order to solve this problem, art to encrypt the transmission path using WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA 2, or the like, which are encryption standards for wireless LAN, have been put into practical use (see Patent Literature 1, for example).

[0004]

Furthermore, in order to prevent the leakage of information transmitted to and received from a terminal without placing a burden on the user, an information processing device that processes data transmitted to and received from a terminal is known depending on the connection type with the terminal (see Patent Literature 2, for example).

[Summary of Invention]

[Problem to Be Solved by Invention]

[0005]

Conventional art makes it difficult for users to easily configure security information while strengthening the prevention of leakage of information from a device.

[0006]

The present invention was made in consideration of the foregoing problem, and an object thereof is to provide a communication device that enables users to easily configure security information while strengthening the prevention of leakage of information.

[Means for Solving Problem]

[0007]

To solve the foregoing problem, a communication device has communication means capable of one-to-one connection with an external device holding certificate information required to connect to a network; acquisition means for acquiring the certificate information from the external device connected by the communication means; and connection request means for sending a request for connection to the network to a communication management device, which performs authentication to determine whether to permit a connection to the network, using the certificate information acquired by the acquisition means.

[Effects of Invention]

[0008]

According to the present invention, it is possible to provide a communication device that enables users to easily configure security information while strengthening the prevention of leakage of information.

[Brief Description of Drawings]

[0009]

FIG. 1 is a schematic diagram of a transmission system according to one embodiment.

FIG. 2 is an external view of a communication device according to one embodiment.

FIG. 3 is a hardware configuration diagram of the communication device according to one embodiment.

FIG. 4 is a hardware configuration diagram of an external input device according to one embodiment.

FIG. 5 is a schematic diagram of a communication system according to a first embodiment.

FIG. 6 is a functional configuration diagram of the communication system according to the first embodiment.

FIG. 7 is a sequence chart illustrating the flow of processing by the communication system according to the first embodiment.

FIG. 8 is an example of a display of login information according to the first embodiment.

FIG. 9 is an example of a display of a login screen according to the first embodiment.

FIG. 10 is an example of a display of a certificate selection screen according to the first embodiment.

FIG. 11 is an example of a display of a result display screen according to the first embodiment.

FIG. 12 is a functional configuration diagram of a communication system according to a second embodiment.

FIG. 13 is an example of a display of ad hoc mode configuration information according to the second embodiment.

FIG. 14 is a functional configuration diagram of a communication system according to a third embodiment.

FIG. 15 is a sequence chart illustrating the flow of processing by the communication system according to the third embodiment.

FIG. 16 is an example of a display of login information according to the third embodiment.

FIG. 17 is an example of a display of a one-time password input screen according to the third embodiment.

FIG. 18 is a functional configuration diagram of a communication system according to a fourth embodiment.

FIG. 19 is a diagram illustrating a configuration example of a communication system according to a fifth embodiment.

FIG. 20 is a diagram illustrating a configuration example of the hardware of the communication system according to the fifth embodiment.

[Description of Embodiments]

[0010]

Embodiments of the present invention are described below with reference to attached drawings.

[0011]

<Overall configuration of transmission system>

FIG 1. is an overall configuration diagram of a transmission system 1 according to one embodiment. The transmission system contains a data provision system for communicating content data in one direction from one transmission terminal to another transmission terminal via a transmission management system, or a communication system for mutually delivering information, emotions, or the like between a plurality of transmission terminals via the transmission management system. This communication system is a system for mutually delivering information, emotions, or the like between a plurality of communication terminals (equivalent to "transmission terminal") via a communication management system (equivalent to "transmission management system"). Examples of this communication system include television or videoconferencing systems, videophone systems, audio conferencing systems, voice telephone systems, PC (personal computer) screen sharing systems, and the like.

[0012]

In the present embodiment, the transmission system, the transmission management system, and the transmission terminal are described on the assumption that a television or videoconferencing system is one example of a communication system, a television or videoconferencing management system is one example of a communication management system, and a television or videoconferencing terminal is one example of a communication terminal. In other words, the transmission terminal and transmission management system according to the present invention are not only applicable to television or videoconferencing systems, but also to communication systems or transmission systems.

[0013]

Transmission system 1 illustrated in FIG. 1 is constructed by a plurality of communication devices (10aa, 10ab, ..., 10db), a display (120aa, 120ab, ..., 120db) for each communication device (10aa, 10ab, ..., 10db), a plurality

of relay devices (30a, 30b, 30c, 30d), a transmission management system 50, a program provision system 90, and a maintenance system 100.

[0014]

Note that in the present embodiment, “communication device 10” is used when indicating any communication device among the communication devices (10aa, 10ab, ..., 10db). Furthermore, “display 120” is used when indicating any display among the displays (120aa, 120ab, ..., 120db), and “relay 30” is used when indicating any relay device among the relay devices (30a, 30b, 30c, 30d).

[0015]

The communication device 10 transmits and receives image data, audio data, or the like to and from another communication device 10. In the present embodiment, an image of image data is described as being a video, but this image may be still an image as well as a video. Furthermore, the image of the image data may include both videos and still images. Note that among the communication devices (10aa, 10ab, ..., 10db), the communication devices 10da and 10db have a wireless LAN interface and are connected to a communication network 2 via a wireless LAN access point 60. Furthermore, a communication management device 80 is an IEEE 802.11X authentication server.

[0016]

The relay device 30 relays image data and audio data between the plurality of communication devices 10. The transmission management system 50 centrally manages the communication device 10 and the relay device 30. An external input device 40 is connected to the communication device 10 and transmits display data for displaying document data to the communication device 10. The document data here refers to data that is utilized using, for example, document creation software, spreadsheet software, presentation software, or the like.

[0017]

Furthermore, a plurality of routers (70a, 70b, ..., 70f) illustrated in FIG. 1 select the optimal path for image data and audio data. Note that in the present embodiment, “router 70” is used when indicating any router among the routers (70a, 70b, ..., 70f). The program provision system 90 is provided with an unillustrated HD (hard disk), within which is stored a communication device program for causing the communication device 10 to implement various functions or various means, and is able to transmit the communication device program to the communication device 10.

[0018]

Furthermore, the HD of the program provision system 90 also stores a relay device program for causing the relay device 30 to implement various functions or various means, and is able to transmit the relay device program to the relay device 30. Moreover, the HD of the program provision system 90 also stores a transmission management program for causing the transmission management system 50 to implement various functions or various means, and is able to transmit the transmission management program to the transmission management system 50.

[0019]

Furthermore, the communication device 10aa, the communication device 10ab, the relay device 30a, and the router 70a are communicably connected by a LAN 2a. The communication device 10ba, the communication device 10bb, the relay device 30b, and the router 70b are communicably connected by a LAN 2b. Furthermore, the LAN 2a and LAN 2b are communicably connected by a dedicated line 2ab that includes the router 70c, and are constructed within a predetermined region A. For example, region A is Japan; LAN 2a is constructed within an establishment in Tokyo, and LAN 2b is constructed within an establishment in Osaka.

[0020]

On the other hand, the communication device 10ca, the communication device 10cb, the relay device 30c, and the router 70d are communicably connected by a LAN 2c. The communication device 10da, the communication device 10db, the relay device 30d, the communication management device 80, and the router 70e are communicably connected by a LAN 2d. Furthermore, the LAN 2c and LAN 2d are communicably connected by a dedicated line 2cd that includes the router 70f, and are constructed within a predetermined region B. For example, Region B is the United States; LAN 2c is constructed within an establishment in New York, and LAN 2d is constructed within an establishment in Washington D.C. Region A and region B are communicably connected via an Internet 2i from their respective routers (70c, 70f).

[0021]

Furthermore, the transmission management system 50 and the program provision system 90 are communicably connected to the communication device 10 and the relay device 30 via the Internet 2i. The

transmission management system 50 and the program provision system 90 may be installed in region A or region B, or may be installed in other regions.

[0022]

Note that in the present embodiment, the communication network 2 according the present embodiment is constructed by the LAN 2a, LAN 2b, dedicated line 2ab, Internet 2i, dedicated line 2cd, LAN 2c, and LAN 2d.

[0023]

Furthermore, in FIG. 1, the four sets of numbers shown under each communication device 10, each relay device 30, the transmission management system 50, each router 70, and the program provision system 90 are simple representations of IP addresses in general IPv4. For example, the IP address of the communication device 10aa is "1.2.1.3." Furthermore, IPv6 may be used instead of IPv4, but to simplify the description, IPv4 will be used herein.

[0024]

<Hardware configuration of communication device>

Next, a hardware configuration of the communication device 10 according to one embodiment will be described.

[0025]

FIG. 2 is an external view of the communication device 10 according to the first embodiment. The following describes the longitudinal direction of the communication device 10 as the X-axis direction, the direction perpendicular to the X-axis direction in the horizontal plane as the Y-axis direction, and the direction perpendicular to the X-axis direction and the Y-axis direction (vertical direction) as the Z-axis direction.

[0026]

As illustrated in FIG. 2, the communication device 10 is provided with a housing 1100, an arm 1200, and a camera housing 1300. Of these, a front wall surface 1110 of the housing 1100 is provided with an unillustrated intake surface formed by a plurality of intake holes, and a back wall surface 1120 of the housing 1100 is provided with an exhaust surface 1121 formed by a plurality of exhaust holes. As a result, external air in front of the communication device 10 may be drawn in through the unillustrated intake surface by the drive of a cooling fan built into the housing 1100 and exhausted to the back of the communication device 10 via the exhaust surface 1121. A sound pickup hole 1131 is formed on a right side wall surface 1130 of the housing 1100, and a built-in microphone 114, which will be described later, is capable of picking up sound such as audio, sound, noise, or the like.

[0027]

An operation panel 1150 is formed on the right side surface 1130 side of the housing 1100. The operation panel 1150 is provided with a plurality of operation buttons (108a to 108e) described below, a power switch 109 described below, and an alarm light 119 described below. Furthermore, an audio output surface 1151 formed by a plurality of audio output holes for passing output audio from a built-in speaker 115 described below is formed. Furthermore, a containment unit 1160 is formed on a left side wall surface 1140 side of the housing 1100 as a recessed portion for containing the arm 1200 and camera housing 1300.

[0028]

A plurality of connections (1132a to 1132c) for electrically connecting a cable to an external device connection I/F 118 described below is provided on the right side wall surface 1130 of the housing 1100. On the other hand, an unillustrated connection for electrically connecting a cable 120c for the display 120 to the external device connection I/F 118 described below is provided on the left side wall surface 1140 of the housing 1100.

[0029]

Note that in the following description, "operation button 108" is used when indicating any operation button among the operation buttons (108a to 108e), and "connection 1132" is used when indicating any connection among the connections (1132a to 1132c).

[0030]

Next, the arm 1200 is attached to the housing 1100 via a torque hinge 1210, and the arm 1200 is configured to be vertically rotatable at a tilt angle $\theta 1$ in a range of 135 degrees relative to the housing 1100. FIG. 2 illustrates a state where the tilt angle $\theta 1$ is 90 degrees.

[0031]

The camera housing 1300 is provided with a built-in camera 1021 that is capable of capturing images of the user, documents, rooms, and the like. Furthermore, a torque hinge 1310 is formed on the camera housing 1300. The camera housing 1300 is attached to the arm 1200 via the torque hinge 1310. Furthermore, when the state illustrated in FIG. 2 is defined as 0 degrees, the camera housing 1300 is configured to be vertically and horizontally rotatable at a panning angle θ_2 in a range of ± 180 degrees and a tilt angle θ_3 in a range of ± 45 degrees relative to the arm 1200.

[0032]

FIG. 3 is a hardware configuration diagram of the communication device 10 according to one embodiment of the present invention. As illustrated in FIG. 3, the communication device 10 includes a common computer configuration, and is provided with, for example, a CPU (Central Processing Unit) 101, ROM (Read Only Memory) 102, RAM (Random Access Memory) 103, flash memory 104, SSD (Solid State Drive) 105, media drive 107, operation button 108, power switch 109, network I/F 111, camera 112, image sensor I/F 113, microphone 114, speaker 115, audio input/output I/F 116, display I/F 117, external device connection I/F 118, alarm light 119, wireless LAN I/F 121, and a bus line 110, such as an address bus, a data bus, or the like, for electrically connecting each of the foregoing constituent elements as illustrated in FIG. 3, or the like.

[0033]

The CPU 101 is an arithmetic device for implementing the various functions that the communication device 10 is provided with by reading a program or data from the ROM 102 or the like and executing processing. The ROM 102 is non-volatile memory for storing a program or the like for the communication device 10, and is constituted by, for example, flash ROM or the like. The RAM 103 is volatile memory used as a work area of the CPU 101. The CPU 101, ROM 102, and RAM 103 execute a program of the communication device 10 as a control unit 122. The flash memory 104 is non-volatile memory for storing various data such as image data, audio data, or the like. The SSD 105 controls the reading or writing of various data to the flash memory 104 according to the control of the CPU 101.

[0034]

The media drive 107 controls the reading or writing (storing) of data to the recording media 106, such as a memory card or the like. The operation button 108 is an input unit for performing the various operations of the communication device 10, and may be input means other than a button, for example, a touch panel or the like. The power switch 109 is a switch for switching the power to the communication device 10 on and off. The network I/F 111 is an interface such as wired LAN or the like for transmitting and receiving data by utilizing a network.

[0035]

The camera 112 is a device for capturing a subject according to the control of the CPU 101, and contains a lens and a solid state image sensor for converting light into an electrical charge and digitizing the image (picture) of the subject. Note that CMOS (Complementary Metal Oxide Semiconductor), CCD (Charge Coupled Device), or the like is used as the solid state image sensor. The image sensor I/F 113 is an interface for capturing an image signal output from the camera 112 for imaging as predetermined image data. The microphone 114 inputs audio and converts it into an audio signal. The speaker 115 converts the input audio signal into audio. The audio input/output I/F captures the audio signal input from the microphone 114 as predetermined audio data according to the control of the CPU 101. Furthermore, output audio data is converted into an audio signal that can be played back by the speaker 115.

[0036]

The display I/F 117 is an interface for outputting various images, for example, communication destination images, menu screens, configuration screens, or the like to the display 120. The display 120 is a display unit constituted by liquid crystal or organic EL for displaying an image of a subject, an icon for operation, or the like. The display 120 is connected to the display I/F 117 by the cable 120c. The cable 120c may be an analog RGB (VGA) signal cable or a component video cable. Furthermore, the cable may be an HDMI (registered trademark) (High-Definition Multimedia Interface) or DVI (Digital Video Interactive) signal cable.

[0037]

Note that the communication device 10 and the display 120 may be integrated. Furthermore, when integrated, the communication device 10 may be provided with a projector configuration instead of the display 120.

[0038]

The external device connection I/F 118 is an interface for transmitting and receiving various data from an external device, and includes, for example, a USB (Universal Serial Bus) or the like. An external device such

as an external camera, an external microphone, an external speaker, or the like may each be connected electrically to the external device connection I/F 118 by a USB cable or the like plugged into the connection 1132 of the housing 1100 illustrated in FIG. 2. When an external camera is connected, the external camera operates with priority over the built-in camera 112 according to the control of the CPU 101. Similarly, when an external microphone is connected or an external speaker is connected, the external microphone or the external speaker operates with priority over the built-in microphone 114 or the built-in speaker 115, respectively, according to the control of the CPU 101.

[0039]

Note that from the viewpoint of security, the external device connection I/F 118 of the communication device 10 is configured to recognize only predetermined devices such as the foregoing external camera, microphone, speaker, and the like. In such a system, data cannot be read or written even when an external USB memory, hard disk device, or the like is connected, so there has been difficulty in importing the certificate information required for connecting to a network into the communication device 10.

[0040]

The alarm light 119 displays an abnormality, operational status, or the like of the various functions of the communication device 10. The wireless LAN I/F 121 is a wireless LAN interface for transmitting and receiving data by utilizing a network. The bus line 110 connects each of the foregoing constituent elements as illustrated in FIG. 3 and conveys the address bus, data bus, various control signals, and the like.

[0041]

Note that the recording media 106 is configured to be easily attachable to and detachable from the communication device 10. Furthermore, provided that the flash memory 104 is non-volatile memory for reading or writing data in accordance with the control of the CPU 101, it may be not limited to flash memory but may also be EEPROM (Electrically Erasable and Programmable ROM) or the like.

[0042]

Furthermore, the foregoing communication device program may be distributed by being recorded in a computer-readable recording medium such as the recording media 106 as a file in an installable or executable format.

[0043]

<Hardware configuration of external input device>

FIG. 4 is a hardware configuration diagram of the external input device 40 according to one embodiment. The external input device 40 has a common computer configuration, and has, for example, a CPU 201, ROM 202, RAM 203, HD (Hard Disk) 204, HDD (Hard Disk Drive) 205, media drive 207, display 208, network I/F 209, keyboard 211, mouse 212, optical drive 214, bus line 210, or the like.

[0044]

The CPU 201 is an arithmetic device for implementing the various functions that the external input device 40 is provided with by reading a program or data from the ROM 202, HD 204, or the like and executing processing. The ROM 202 is non-volatile memory for storing a program or the like for the external input device 40, and is constituted by, for example, flash ROM or the like. The RAM 203 is volatile memory utilized as a work area of the CPU 201.

[0045]

The HD 204 saves various software, data, image data, audio data, or the like required for the various processing executed by the CPU 201. The HDD 205 controls the reading or writing of various data to the HD 204 according to the control of the CPU 201. The media drive 207 controls the reading or writing of data to the media 206, which is, for example, recording media such as a memory card or the like. The display 208 displays various information such as a cursor, menu, window, text, image, video, and the like. Note that the display 208 may be provided external to the external input device.

[0046]

The network I/F 209 is an interface for transmitting and receiving data via a network, and includes, for example, a wired LAN and/or a wireless LAN or the like. The keyboard 211 inputs characters and the like. The mouse 212 is a means of selecting and executing various instructions, selecting a target to be processed, moving a cursor, or the like, and may be another pointing device such as, for example, a touch panel, touch pad, or the like. The optical drive 214 controls the reading or writing of data to an optical disc, for example, a CD (Compact Disc), DVD, Blu-ray, or the like.

[0047]

The external device I/F 215 is an interface for inputting and outputting various data to and from an external device, and includes, for example, a USB interface or the like. The bus line 210 conveys the address bus, data bus, various control signals, or the like.

[0048]

Note that an external input device program for controlling the external input device 40 is recorded in the ROM 202. The external input device program may be distributed by being recorded in a computer-readable recording medium as a file in an installable or executable format.

[0049]

[First embodiment]

The present embodiment relates to the configuration of security information for a communication device connected to a network by wireless LAN or the like. In the present embodiment, WPA (Wi-Fi Protected Access)/WPA2-Enterprise mode is described as an example of authentication art used in configuring wireless communication. Note that there is another WPA/WPA2 mode: Home (WPA-PSK) mode. WPA/WPA2-Enterprise mode is for businesses, whereas WPA/WPA2 Home mode is often used by individuals, small offices, and the like.

[0050]

In WPA/WPA2-Enterprise mode, for example, authentication of a user (communication device) is performed using an IEEE 802.1X-compatible authentication server or the like. In IEEE 802.1X, for example, the communication device is authenticated using an authentication protocol called EAP (Extensible Authentication Protocol), or the like. Then, if authentication is successful, the communication device is permitted to connect to the network, and if authentication fails, the communication device is not permitted to connect to the network.

[0051]

There are multiple methods for EAP, but in the present embodiment, the user (communication device) is authenticated using a digital certificate.

[0052]

<System configuration>

FIG. 5 is a configuration diagram of a communication system 500 according to the first embodiment. The communication system 500 has communication devices 10da and 10db, external input devices 40da and 40db, access points 60a and 60b for a LAN (Local Area Network) 501, and a communication management device 80. Furthermore, the communication devices 10da and 10db are connected to displays 120da and 120db, respectively.

[0053]

The access points 60a and 60b are installed, for example, in conference rooms 502 and 503, respectively, in a predetermined building. The access points 60a and 60b communicate wirelessly with the communication devices 10da and 10db, respectively. The communication method of this wireless communication is, for example, a wireless LAN system standardized by IEEE 802.11. Note that in IEEE 802.11, several methods such as IEEE 802.11b/a/g/n or the like are standardized, but the method is not specified in the present embodiment. Furthermore, access points 60a and 60b are compatible with standards such as WPA/WPA2-Enterprise mode, IEEE 802.1X, or the like.

[0054]

The communication devices 10da and db are terminals for teleconferencing, for example, and are connected to the LAN 501, communication network 2, or the like via the access points 60a and 60b or the like, and communicate with other communication devices or the like. The communication devices 10da and 10db are configured to be capable of communicating with access points 60b and 60a by at least one of one or a plurality of wireless LAN standards supported by the access points 60a and 60b. Furthermore, the communication devices 10da and db are compatible with standards such as WPA/WPA2-Enterprise mode, IEEE 802.1X, or the like.

[0055]

The external input devices 40da and 40db are, for example, notebook PCs, and are capable of communicating with the communication devices 10da and 10db, respectively, via a predetermined communication method. Note that the external input devices 40da and 40db are not limited to notebook PCs, but may also be information processing devices such as desktop PCs, smartphones, tablet terminals, or the like. Note that the

foregoing predetermined communication method between the external input devices 40da and 40db and the communication devices 10da and 10db is, for example, peer-to-peer connection using a crossover LAN cable or interconnection using wireless LAN ad hoc mode or the like.

[0056]

Here, interconnection refers to a one-to-one mutual connection between the communication device 10 and the external input device 40 without a server or the like. In addition to the above-described peer-to-peer connection using a crossover LAN cable or the like, a connection using wireless LAN ad hoc mode or the like, or the like, specific examples of interconnection include, for example, one-to-one connection using short-range wireless communication such as Bluetooth (registered trademark) or the like.

[0057]

The external input devices 40da and 40db hold the certificate information required to connect to a network such as LAN 501, the communication network 2, or the like. Note that the external input devices 40da and 40db are one example of the external device according to the present invention.

[0058]

For example, the communication management device 80 is a server device connected to a network such as LAN 501, the communication network 2, or the like, and performs authentication to determine whether to permit a connection to the network in response to a connection request from the communication device 10da, 10db, or the like to the network.

[0059]

<Functional configuration>

Next, the functional configuration of the communication system 500 will be described using FIG. 6. FIG. 6 is a functional configuration diagram of the communication device 10da, the external input device 40da, the access point 60a, and the communication management device 80. Note that the communication device 10db in FIG. 5 has the same function as the communication device 10da, and the access point 60b has the same function as the access point 60a.

[0060]

The communication device 10da has wireless communication means 601, wired communication means 602, display means 603, acquisition means 604, connection request means 605, storage means 606, and input means 607.

[0061]

The wireless communication means 601 is a means of transmitting and receiving data by wireless LAN standardized by, for example, IEEE 802.11 or the like, and includes, for example, the wireless LAN I/F 121 in FIG. 3 and software or the like for controlling the same. The wired communication means 602 is a communication means that is capable of one-to-one interconnection with the external input device 40da without the LAN 501, a server, or the like, for example, by a peer-to-peer connection with the external input device 40da via a crossover LAN cable or router or the like.

[0062]

The wired communication means 602 includes, for example, the network I/F 111 in FIG. 3 and control software thereof or the like. Note that the wired communication means 602 also functions as an ordinary LAN interface by connecting to a network such as LAN 501 or the like by a straight LAN cable.

[0063]

The display means 603 is a means of displaying login information, which is the authentication information required when logging in to the communication device 10da from the external input device 40da interconnected to the wired communication means 602. The display means 603 includes, for example, the display 120 in FIG. 3, the display I/F 117, and the control software thereof or the like.

[0064]

The acquisition means 604 is a means of acquiring the certificate information required to connect to the network by the wireless communication means 601 from the external input device 40da connected by the wired communication means 602, and, for example, this is implemented by a program that is operated by the control unit 122 in FIG. 3 or the like. Furthermore, the acquisition means 604 has server means 608, login authentication means 609, and password generation means 610.

[0065]

The password generation means 610 is a means of generating the password included in the login information displayed by the display means 603. In the present embodiment, the password generation means 610 generates a one-time password that is different information each time it is displayed by the display means 603. The server means 608 provides a web page for entering login information, such as the one-time password displayed by the display means 603, or the like, via the wired communication means 602.

[0066]

The login authentication means 609 authenticates whether the login is permitted using the login information, which is the authentication information displayed by the display means 603. The login authentication means 609, for example, permits the login of the external input device 40da when the login information entered on the web page provided by the server means 608 contains the one-time password displayed by the display means 603.

[0067]

When the correct one-time password is input from the external input device 40da and the login is permitted, the connection request means 605 requests the communication management device 80 to connect to the network by the wireless connection means 601 using the certificate information acquired by the acquisition means 604. The storage means 606 is a means of storing the certificate information acquired by the acquisition means 604, an encryption key that is notified when authentication by the communication management device 80 is successful, or the like, and, for example, is included in the RAM 103 or flash memory 104 in FIG. 3, or the like. The input means 607 is a means by which a user of the communication device 10da operates the communication device 10da, enters a key, or the like, and includes, for example, the operation panel in FIG. 3.

[0068]

According to the foregoing configuration, the communication device 10da causes the display means 603 to display the login information containing the one-time password. Then, the server means 608 causes the external input device 40da that is interconnected to the wired communication means 602 to display a web page on which to enter login information. When login information is entered on the web page, the login authentication means 609 determines whether the input login information contains the one-time password displayed by the display means 603. Then, logging in to the external input device 40da is permitted when the correct one-time password is contained.

[0069]

The acquisition means 604 acquires the certificate information used for network authentication from the external input device 40da. Then, when logging in to the external input device 40da is permitted, the connection request means 605 requests the communication management device 80 to connect to the network by the wireless connection means 601 using the certificate information acquired by the acquisition means 604. When permitted to connect to the network by the communication management device 80, the communication device 10da is able to connect wirelessly to the network to which connection is permitted by the wireless communication means 601.

[0070]

As a result of the foregoing operation, the communication device 10da is able to acquire the certificate information required for network authentication safely and easily from the external input device 40da, that is, to perform the communication configuration.

[0071]

Next, the functional configuration of the external input device 40da will be described. The external input device 40da has communication means 611, certificate storage means 612, control means 613, operation input means 614, and screen display means 615. The communication means 611 is a means of transmitting and receiving data using a wired LAN interface, and is capable of interconnection with the communication device 10da without a network such as LAN 501 or the like, by peer-to-peer connection via a crossover LAN cable, hub, or the like. Note that the communication means 611 may, for example, be a general wired LAN interface provided by a computer.

[0072]

The certificate storage means 612 is a means of storing certificate information such as a digital certificate or the like used when authenticating between the communication management device 80 using, for example, EA-TLS (Transport Layer Security) or the like, and is contained in the HD 204, RAM 203, or the like in FIG. 4. The digital certificate, for example, is specified by X.509 of ITU-T (International Telecommunication Union-

Telecommunication sector). The digital certificate contains, for example, a digital signature algorithm, issuer name, expiration date, user name, public key information of the user, and the like.

[0073]

The control means 613 is a means of executing various programs of the external input device 40da, and includes, for example, the CPU 201, ROM 202, RAM 203, or the like in FIG. 4. The control means 613 has certificate management means 616 and browser means 617.

[0074]

The certificate management means 616 is a means of managing certificates stored in the certificate storage means 612, and, for example, certificate information acquired from a certificate authority is stored in the certificate storage means 612. Furthermore, it has a function of transmitting the certificate information stored in the certificate storage means 612 to the communication device 10da connected via the communication means 611, or the like.

[0075]

The browser means 617 causes the screen display means 615 to display a web page provided by the communication device 10da connected via the communication means 611, and transmits login information such as a one-time password or the like input to the web page from the operation input means 614 or the like to the communication device 10da.

[0076]

Next, the communication management device 80 and access point 60a will be described. Note that since the communication management device 80 and access point 60a are well-known art, only an outline will be described.

[0077]

The communication management device 80 is, for example, a server device or the like that has the hardware configuration of a general computer, and has a transmission/reception unit 622, an authentication management database 623, and an authentication unit 621. The transmission/reception unit 622 connects the communication management device 80 to the network and transmits and receives data. The authentication management database 623 stores digital certificates issued by a certificate authority. The authentication unit 621 authenticates the user (communication device) requesting connection based on the authentication management database 623. The communication management device 80 is an authentication server that authenticates communication devices 10a, 10db, and the like that request connection to the network, and, for example, is known as an IEEE 802.1X RADIUS (Remote Authentication Dial-in User Service) authentication server.

[0078]

The access point 60a has a wired transmission/reception unit 618, a connection unit 619, and a wireless transmission/reception unit 620. The wired transmission/reception unit 618 is connected to a network such as LAN 501 or the like and transmits data to and from a device such as the communication management device 80 or the like connected to the network. The wireless transmission/reception unit 620 transmits data to and from a wireless LAN terminal such as the communication device 10da or the like. The connection unit 619 controls the connection between the wired transmission/reception unit 618 and the wireless transmission/reception unit 620.

[0079]

When connected to the access point 60a, the communication device 10da transmits a connection request including the certificate information to the communication management device 80. This connection request is forwarded by the access point 60a to the communication management device 80. Note that at this time, packet conversion or the like is performed at the access point 60a, and the authentication itself is performed between the communication device 10da and the communication management device 80.

[0080]

The communication management device 80 authenticates the certificate information contained in the connection request from the communication device 10da based on the authentication management database 623. If authentication is successful in the communication management device 80, the communication management device 80 notifies access point 60a that the authentication was successful. The connection unit 619 of access point 60a that received the notification permits the communication device 10da to communicate with the network. On the other hand, if authentication fails, the connection unit 619 will not permit the communication device 10da to communicate with the network. That is, the connection unit 619, with the

exception of connection requests, blocks communication from non-authorized communication devices and permits communication of authorized communication devices.

[0081]

Next, a summary of the operation of the communication system 500 will be described using FIG. 7. FIG. 7 is a sequence chart illustrating the flow of processing by the communication system 500 according to the first embodiment. When an input is received instructing the start of wireless communication configuration from the input means 607 or the like, the communication device 10da starts processing the wireless communication configuration. Note that the input from the input means 607 is one example; for example, the processing may be started when the external input device 40da is interconnected to the wired communication means 602 by a crossover LAN cable or the like.

[0082]

The acquisition means 604 of the communication device 10da generates a one-time password using the password generation means 610. Furthermore, login information containing the generated one-time password, the URL (Uniform Resource Locator) of the connection destination, and the like is displayed by the display means 603 (step S701). FIG. 8 illustrates an example of the display of login information. In FIG. 8, the communication device 10da, for example, displays a URL 801 of the connection destination and a one-time password 802 on the display 120 in FIG. 3. The URL 801 of the connection destination indicates the address of the login web page provided by the server means 608 of the communication device 10da.

[0083]

Returning to FIG. 7, the browser means 617 of the external input device 40da accepts the input of the URL of the connection destination from the operation input means 614 (step S702). This input is made by the user, and the content is assumed to be the URL 801 of the connection destination displayed in step S701. When the URL input is accepted, the browser means 617 transmits a connection request to the communication device 10da via the communication means 611 using the HTTPS protocol (HyperText Transfer Protocol over Secure Socket Layer) with respect to the input URL (step S703).

[0084]

Note that if the communication device 10da has connection means to a network such as a LAN port or the like other than the communication means 611, there is a possibility that the connection means to a network other than the communication means 611 is connected to the Internet. In this case, an attack such as communication interception, spoofing, or the like from the Internet is a concern. In the present embodiment, the communication path between the communication device 10da and the external input device 40da via interconnection is encrypted by HTTPS protocol to protect information from communication interception or a spoofing attack. In other words, security (safety) is improved. Furthermore, as a more suitable example, the external input device 40da may have a function to disable communication means other than communication means 611 while in communication with the communication device 10da by the communication means 611.

[0085]

When a connection request is received from the external input device 40da (step S704), the server means 608 of the communication device 10da transmits the HTML (Hyper Text Markup Language) of the login screen to the external input device 40da (step S705). The browser means 617 of the external input device 40da causes the screen display means 615 to display the login screen and accepts a one-time password input by the user (step S706).

[0086]

FIG. 9 illustrates an example of the display of a login screen 901 displayed by the browser of the external input device 40da. In FIG. 9, a one-time password input field 902 and a login button 903 are displayed on the login screen 901. It is assumed that the user will enter the one-time password displayed by the display means 603 of the communication device 10da in the one-time password input field 902. When the user enters the one-time password in the input field 902 and presses the login button 903, the browser means 617 transmits a login request containing the input one-time password to the communication device 10da (step S707).

[0087]

When the acquisition means 604 of the communication device 10da receives a login request from the external input device 40da, the login authentication means 609 compares the one-time password contained in the login request with the one-time password generated by the password generation means 610. If the one-time password for the login request and the one-time password generated by the password generation means 610 match, the login is permitted, and if they do not match, the login is rejected (step S708).

[0088]

This login authentication processing prevents the acquisition means 604 from processing requests from a third party other than the external input device 40da. As a result, communication by the user of the external input device 40da may be guaranteed, so the communication device 10da may import the certificate information safely. Furthermore, since the login information is a one-time password in the present embodiment, security may be further strengthened.

[0089]

If the login authentication means 609 permits the login of the external input device 40da, the server means 608 transmits HTML for causing the browser of the external input device to display a certificate selection screen via the wired communication means 602 (step S709). FIG. 10 illustrates an example of the display of a certificate selection screen 1001 displayed by the browser of the external input device 40da. The user presses a browse button 1002, selects the certificate file, and then presses a transmit button 1003. Accordingly, the certificate management means 616 reads the certificate information (certificate file) from the certificate storage means 612 (step S710) and transmits the read certificate information to the communication device 10da (step S711).

[0090]

The acquisition means 604 of the communication device 10da stores the certificate information received by the server means 608 from the external input device 40da in the storage means 606 (step S712). The server means 608 transmits the HTML for displaying the transmission result on the browser of the external input device 40da to the external input device 40da via the wired communication means 602 (step S713). FIG. 11 illustrates an example of the display of a result display screen 1101 displayed by the browser of the external input device 40da. In FIG. 11, the transmitted result (success) 1102 is displayed on the result display screen 1101. Note that if the transmitted result fails, that fact is displayed as the transmitted result 1102.

[0091]

Next, the connection request means 605 of the communication device 10da reads the certificate information from the storage means 606 (step S714). Furthermore, the connection request means 605 transmits a connection permission request containing the read certificate information to the communication management device 80 via the wireless communication means 601 and access point 60a (step S715).

[0092]

The connection unit 619 of the access point 60a receives the connection request received from the communication device 10da via the wireless transmission/reception unit 620 and transmits the same to the communication management device 80 as a connection availability request via a priority transmission/reception unit 618 (step S716). Note that at this time, the access point 60a forwards the connection request, and the authentication process itself is performed between the communication device 10da and the communication management device 80.

[0093]

When the connection availability request containing certificate information is received from the access point 60a via the transmission/reception unit 622, the authentication unit 621 of the communication management device 80 queries the authentication management database 623 and performs authentication processing (step S717). Next, the authentication unit 621 notifies the access point 60a of the authentication result via the transmission/reception unit 622 (step S718).

[0094]

When the authentication result with respect to the connection availability request is received from the communication management device 80, the connection unit 619 of the access point 60a confirms the authentication result, and if authentication is successful, permits the communication device 10da to connect to the network (step S719). As a result, the communication device 10da is connected to the network and capable of communicating, for example, with a communication device or the like installed at another site (step S720). In other words, preparations are made to hold a remote conference via wireless communication. On the other hand, if the authentication result fails, the connection unit 619 will not permit the communication device 10da to connect to the network.

[0095]

Note that the communication device 10da stores the certificate information acquired from the external input device 40da in the storage means 606, such as flash memory or the like, in FIG. 3; however, after connecting to the network, the stored certificate information authentication may be erased from the storage means 606.

By erasing the certificate information from the storage means 606, it is possible to prevent unauthorized reading or the like of the certificate.

[0096]

Furthermore, when connected to the network, the communication device 10da may delete the certificate information in the storage means 606 after registering information related to the certificate information in another secure area, for example, a registry or the like. In this case, the communication device 10da is able to connect to the network again based on the information registered in the registry or the like, even if the certificate information stored in the storage means 606 is deleted.

[0097]

Moreover, as a suitable example, the communication device 10da may delete or invalidate the certificate information acquired from the external input device 40da according to predetermined conditions, such as after the communication is completed, after the power is turned off, or when the user performs a predetermined operation. In this case, when connecting to the network again, it is necessary to import the certificate information from the external input device 40da again, and therefore leakage or the like of information due to unauthorized use of the terminal by a third party may be effectively prevented.

[0098]

According to the present embodiment above, the certificate required for network connection may be imported safely and easily from the external input device 40da. Specifically, the certificate required for wireless LAN connection may be imported safely and easily by utilizing the wired communication means 602, such as a wired LAN port or the like, of the communication device 10da. Furthermore, by interconnecting the communication device 10da and the external input device 40da using a crossover LAN cable or the like and without a server or the like, communication interception or spoofing by a third party may be reduced.

[0099]

Moreover, the communication device 10da has the login authentication means 609 and performs login authentication of the external input device 40da, and therefore it is possible to import certificates more securely. Moreover, the communication device 10da has the password generation means 610 and performs login authentication using a one-time password generated by the password generation means 610, and therefore it is possible to further strengthen security.

[0100]

[Second embodiment]

In the first embodiment, the communication device 10da and the external input device 40da are described as being interconnected by a crossover cable or the like, but the interconnection between the communication device 10da and the external input device 40da may be by wireless communication.

[0101]

FIG. 12 is a functional configuration diagram of a communication system according to the second embodiment. In FIG. 12, the communication device 10da has second wireless communication means 1201 instead of the wired communication means 602 in the form depicted in FIG. 6. Furthermore, in FIG. 12, the external input device 40da has third wireless communication means 1202 instead of the communication means 611 in FIG. 6, or in addition to the communication means 611. Note that the other configuration is the same as the first embodiment, so here, the description will be focused on the differences from the first embodiment.

[0102]

The second wireless communication means 1201 and third wireless communication means 1202 are means of transmitting and receiving data by wireless LAN standardized by, for example, IEEE 802.11 or the like, and are configured to be capable of interconnection in ad hoc mode.

[0103]

Note that in order to connect the communication device 10da and external input device 40da in ad hoc mode, it is necessary to configure the network connection information. In the present embodiment, the communication device 10da causes the display means 603 to display the configuration information of ad hoc communication mode. FIG. 13 illustrates an example of the display of ad hoc mode configuration information.

[0104]

In FIG. 13, the communication device 10da displays on the display 120 in FIG. 3 information required for ad hoc mode communication configuration, such as, for example, a network name 1301, a security key 1302, or the like of the communication device 10da. After that, the user is able to perform wireless interconnection in

ad hoc mode by inputting the network name 1301 and the security key 1302 displayed on the communication device 10da into the network configuration screen of the external input device 40da.

[0105]

Furthermore, as a more suitable example, the communication device 10da may change the value of security key 1302 each time the ad hoc mode configuration information illustrated in FIG. 13 is displayed, and it is thereby possible to further increase security.

[0106]

After communication in ad hoc mode between the communication device 10da and the external input device 40da has been established by the foregoing operation, connection to the network by the wireless communication means 601 may be performed according to the sequence chart in FIG. 7, as in the first embodiment.

[0107]

According to the present embodiment above, communication between the communication device 10da and the external input device 40da may be established without the use of a crossover cable. Therefore, smartphones, tablets, or the like that generally do not have a wired LAN port may be used as the external input device 40da.

[0108]

Note that wireless LAN is one example of the communication method of the second wireless communication means 1201 and third wireless communication means 1202, and this does not limit the scope of the present invention. For example, the communication method of the second radio communication means 1201 and third radio communication means 1202 may be wireless communication such as Bluetooth, UWB (Ultra-Wide Band), or the like.

[0109]

Furthermore, when the interconnection between the communication device 10da and external input device 40da is wireless LAN, the communication device 10da does not necessarily have to have two wireless LAN interfaces. For example, the wireless LAN I/F 121 in FIG. 3 may be shared by the wireless communication means 601 (first wireless communication means) and second wireless communication means 1201. Alternatively, the communication device 10da may be connected to the network using the second wireless communication means 1201 that has acquired the certificate information by interconnection with the external input device 40da, without being provided with the wireless communication means 601. Moreover, in FIG. 12, the wireless communication means 601 of the communication device 10da may be wired communication means.

[0110]

[Third embodiment]

FIG. 14 is a functional configuration diagram of a communication system 1400 according to the third embodiment. In the present embodiment, the communication device 10da and external input device 40da have first NFC (Near Field Communication) communication means 1401 and second NFC communication means 1402, which are each communication means using NFC.

[0111]

The first NFC communication means 1401 and second NFC communication means 1402 perform non-contact short-range wireless communication (hereinafter referred to as NFC communication) according to the NFC standard. The first NFC communication means 1401 of the communication device 10da receives predetermined data from the second NFC communication means 1402 by NFC communication when the second NFC communication means 1402 of the external input device 40da approaches communication range (for example, within 10 cm). At this time, the communication device 10da must confirm that a communication partner using NFC communication is the correct communication partner. In the present embodiment, the communication device 10da uses a one-time password to authenticate the communication partner using NFC communication, as in the first and second embodiments.

[0112]

FIG. 15 is a sequence chart illustrating the flow of processing by the communication system according to the third embodiment. For example, when an input is received from the input means 607 or the like to instruct the start of wireless communication configuration, the communication device 10da causes the display means 603 to display a one-time password generated by the password generation means 610 (step S1501). One example

of the screen displayed at this time is illustrated in FIG. 16. In FIG. 16, the communication device 10d, for example, displays a one-time password 1601 on the display 120 in FIG. 3.

[0113]

Next, the external input device 40da accepts the input of the one-time password (step S1502). Specifically, the control means 613 of the external input device 40da causes the screen display means 615 to display a one-time password input screen, for example, as illustrated in FIG. 17. In the example in FIG. 17, a password input field 1701, multiple certificate input keys 1702 and 1703, an OK input key 1704, and a clear input key 1705 are displayed on the display 208 of the external input device 40da. The user inputs the one-time password displayed by the communication device 10da in the password input field 1701 using, for example, a mouse 212, keyboard 211, or the like in FIG. 4. Furthermore, if there is a plurality of certificate information, the certificate input keys 1702 and 1703 are displayed, allowing the user to select a certificate. Furthermore, the OK input key 1704 to confirm input and clear input key 1705 to clear input may be displayed. Moreover, the input of other information such as a user ID or the like may be requested as necessary.

[0114]

After the user inputs the one-time password displayed by the communication device 10da into the password input field 1701, the second NFC communication means 1402 of the external input device 40da is brought close to the first NFC communication means 1401 of the communication device 10da, upon which NFC communication is established. When NFC communication is established, the second NFC communication means 1402 of the external input device 40da transmits at least authentication information containing the one-time password input by the user to the first NFC communication means of the 10da communication device (step S1503).

[0115]

On the other hand, when the communication device 10da receives the foregoing authentication information, the login authentication means 609 compares the one-time password contained in the authentication information with the one-time password generated by the password generation means 610 (step S1504). If the one-time password in the authentication information and the one-time password generated by the password generation means 610 match, the communication device 10da transmits the authentication result indicating that authentication was successful to the external input device 40da (step S1505).

[0116]

Note that if the one-time password contained in the authentication information and the one-time password generated by the password generation means 610 do not match, the communication device 10da transmits the authentication result indicating that authentication was dismissed to the external input device 40da. The external input device 40da that received the authentication result indicating that authentication was dismissed causes the screen display means 615 to display that an error was generated, and terminates processing.

[0117]

If the external input device 40da receives the authentication result indicating that authentication was successful from the communication device 10da, the certificate management means 616 reads from the certificate storage means 612 certificate information specified by, for example, the certificate key 1702, 1703, or the like (step S1506). Moreover, the certificate management means 616 transmits the read certificate information to the communication device 10da via the second NFC communication means (step S1507).

[0118]

The acquisition means 604 of the communication device 10da stores the certificate information received from the external input device 40da in the storage means 606 (step S1508). Continuing, the connection request means 605 of the communication device 10da reads the certificate information from the storage means 606 (step S1509). Moreover, the connection request means 605 transmits a connection permission request containing the read certificate information to the communication management device 80 via the wireless communication means 601 (step S1510). The access point 60a forwards the connection permission request from the communication device 10da to the communication management device 80 as a connection availability request (step S1511).

[0119]

When a connection availability request containing certificate information is received from the access point 60a via the transmission/reception unit 622, the authentication unit 621 of the communication management device 80 queries the authentication management database 623 and performs authentication processing (step S1512). Next, the authentication unit 621 notifies the access point 60a of the authentication result via the transmission/reception unit 622 (step S1513).

[0120]

When the authentication result with respect to the connection availability request is received from the communication management device 80, the connection unit 619 of the access point 60a confirms the authentication result, and if authentication is successful, permits the communication device 10da to connect to the network (step S1514). As a result, the communication device 10da is connected to the network and is capable of communicating, for example, with a communication device or the like installed at another site (step S1515).

[0121]

According to the present embodiment above, the certificate required for wireless LAN connection may be imported safely and easily by using the communication device 10da and NFC communication means of the external input device 40da.

Moreover, the communication device 10da has the login authentication means 609 and a password generation means 610, and because authentication is performed using a one-time password generated by the password generation means 610, communication interception or spoofing by a third party may be reduced.

[0122]

(Variation)

In the third embodiment, an example of a case of communicating certificate information by NFC communication was described, but it is also possible to use NFC communication, for example, to configure ad hoc mode between the second wireless communication means 1201 and third wireless communication means 1202 in FIG. 14.

[0123]

For example, in step S1506 in FIG. 15, instead of reading the certificate information required to connect to the network, the connection configuration information (SSID, security key, or the like) of the third radio communication means in FIG. 14 is read, and the read connection configuration information is transmitted to the communication device 10da. The communication device 10da configures ad hoc mode between the second wireless communication means 1201 and third wireless communication means 1202 based on the connection configuration information received from the external input device 40da by NFC communication.

[0124]

The foregoing operation may facilitate ad hoc mode connection configuration using wireless LAN between the communication device 10da and the external input device 40da.

[0125]

Note that ad hoc mode using wireless LAN is one example of interconnection by wireless communication, and it goes without saying that facilitating connection configuration by NFC may be applied to other wireless methods such as, for example, Bluetooth, UWB, or other connection configurations.

[0126]

[Fourth embodiment]

In the first to third embodiments, a case is described where the connection to the network such as LAN 501, the communication network 2, or the like is a wireless LAN connection using the wireless communication means 601. However, IEEE 802.1X is a protocol that specifies authentication for wired LAN and wireless LAN, and therefore the present invention may also be applicable to the case of network connection using wired LAN.

[0127]

FIG. 18 is a functional configuration diagram of a communication system 1800 according to the fourth embodiment. The communication device 10da of the present embodiment has second wired communication means 1801 instead of the wireless communication means 601 of the first embodiment. Furthermore, it has an IEEE 802.1X-compatible switch 1802 instead of the access point 60a according to the first embodiment.

[0128]

The second wired communication means is a means of transmitting and receiving data through a network such as LAN 501 or the like and a wired LAN, and includes, for example, the network I/F 111 in FIG. 3 and control software thereof or the like. The IEEE 802.1X-compatible switch has the same function as the access point 60a in the wireless LAN, connects a device authenticated by the communication management device 80 to the network, and controls unauthenticated devices from connecting to the network.

[0129]

The flow of processing according to the present embodiment may be the same as that of the first embodiment, except that the access point 60a in FIG. 7 is replaced with the IEEE 802.1x-compatible switch.

[0130]

According to the present embodiment above, the certificate required for wired LAN connection may be imported safely and easily.

[0131]

Note that the foregoing configuration is one example and does not limit the scope of the present invention. For example, the communication device 10da does not necessarily have to have two wired LAN interfaces, and the network I/F 111 in FIG. 3 may be shared by the wired communication means 602 and the second wired communication means 1801. Alternatively, the communication device 10da may be connected to the network using the wired communication means 602 that acquires the certificate information by interconnection with the external input device 40da and without being provided with the second wired communication means 1801.

[0132]

Furthermore, for example, in FIG. 18, when importing a certificate from the external input device 40da by the wired communication means 602 (first communication means), control to disable the second wired communication means 1801 (second communication means) may be added. For example, in the sequence chart in FIG. 7, before step S701 in which login information is displayed, it is best to disable communication means other than the communication means that performs interconnection with the external input device 40da. Furthermore, if necessary, after step S720 to connect to the network, a process for re-enabling the disabled communication means may be added.

[0133]

By disabling communication means other than the communication means of importing a certificate from the external input device 40da in this manner, the risk of certificate information being stolen via another communication means such as, for example, the second wired communication means 1801 or the like is eliminated. Therefore, the communication device 10da is then able to establish communication with the network more securely.

[0134]

Furthermore, the user may be prompted to perform an operation that disables the communication means. For example, when the communication device 10da is interconnected with the external input device 40da, means of detecting whether another wired communication means of the communication device 10da is enabled or disabled is provided. Then, when the communication device 10da and the external input device 40da are interconnected and if it is detected that another wired communication means is enabled, a message displaying this fact is displayed and the user may be prompted to perform an operation to disable the other wired communication means.

[0135]

[Fifth embodiment]

The present invention may be applied to various devices and systems having a communication function. For example, the communication device 10 may be used as a car navigation device having a communication function. In the present embodiment, an example of a case when the communication device 10 is adopted as a car navigation device is described.

[0136]

FIG. 19 is a diagram illustrating a configuration example of a communication system according to the fifth embodiment. Note that the basic configuration is the same as the first embodiment, so here the description will focus on the differences.

[0137]

In FIG. 19, a communication system 1900 has, for example, communication devices 10da and 10db, which are car navigation devices installed in cars 1901, 1902, or the like, external input device 40a and 40b, access points 60a and 60b, a communication management device 80, and the like.

[0138]

In the present embodiment, access points 60a and 60b are assumed to be a base station, access point, or the like for a wireless communication system such as, for example, wireless LAN, WiMAX (registered trademark),

a cellular phone, or the like. The communication management device 80 is a device such as a server or the like connected to the communication network 2, and performs authentication to determine whether to permit a connection to the communication network 2 with respect to a connection request from the communication device 10da, 10d, or the like to the communication network 2. The communication devices 10da and 10db are car navigation devices capable of wireless communication with the access point 60a, access point 60b, or the like. When authentication is permitted by the communication management device 80, the communication devices 10da and 10db are capable of performing data communication and the like using the communication network 2 via an access point such as the access point 60a, the access point 60b, or the like. Note that the number of access points in FIG. 19 is one example, and the communication system 1900 may have even more access points.

[0139]

FIG. 20 is a diagram illustrating a configuration example of the hardware of the communication system according to the fifth embodiment. Note that the basic configuration is the same as the hardware configuration diagram of the communication device 10 illustrated in FIG. 3, so here the description will focus on the differences.

[0140]

In FIG. 20, the communication device 10 has a GPS (Global Positioning System) receiver 2101, a vehicle speed sensor 2102, a gyro sensor 2103, or the like in addition to the configuration in FIG. 3. Moreover, the communication device 10 has a wireless communication I/F 2104 for performing wireless communication using the communication method compatible with access points 60a and 60b, instead of the wireless LAN I/F 121 in FIG. 3. Furthermore, in FIG. 20, the communication device 10 has the display 120 built in.

[0141]

Note that in FIG. 20, the network I/F 111 and alarm light 119 from FIG. 3 are omitted, but the communication device 10 may have the network I/F 111 and alarm light 119.

[0142]

For example, by executing a program saved in a ROM 102, a flash memory 104, a media 106, or the like, a control unit 122 causes the communication device 10 to function as a car navigation device. Furthermore, by executing the program in the same manner, the control unit 122 causes the communication device 10 to function as each means for the communication device 10da illustrated in the functional configuration diagram in FIG. 6.

[0143]

The GPS receiver 2101 captures a GPS satellite and outputs the coordinates of its current position. The vehicle speed sensor 2102 is a sensor for detecting the speed of a vehicle (rotation speed of its wheels). The gyro sensor 2103 is a sensor for detecting angular velocity, and by integrating the angular velocity, it is possible to detect the direction of travel of the vehicle.

[0144]

Road map data or the like are saved in the flash memory 104, media 106, or the like. The road map data, for example, are data that represent a road as a combination of nodes and links, and may be downloaded externally. The road map is displayed on the display 120.

[0145]

Furthermore, the communication device 10 may have an audio function for outputting music, a TV broadcast, or the like. Moreover, it may have a browser function for displaying a website.

[0146]

In the foregoing configuration, the communication device 10 estimates the position of the vehicle by applying autonomous navigation, which accumulates the travel distance detected by the vehicle speed sensor 2102 in the travel direction detected by the gyro sensor 2103, based on the position information detected by the GPS receiver 2101. The position the vehicle is displayed on a road map by a vehicle mark or the like.

[0147]

Furthermore, the communication device 10 performs one-to-one interconnection with the external input device 40 by wired or wireless means via the external device connection I/F 118, and is able to acquire authentication information such as certificate information or the like necessary for connecting from the external input device 40 to the communication network 2. For example, the communication device 10 acquires the certificate information from the external input device 40 according to the procedure in the sequence chart in FIG. 7, and

uses the acquired certificate information to request the communication management device 80 to connect to the communication network 2. When authentication by the communication management device 80 is successful, the communication device 10 may be connected to the communication network 2 using the wireless communication I/F 2104. The communication device 10 connected to the communication network 2 is capable of transmitting and receiving various data in the same manner as the communication device 10 in an office, except that it is installed in a mobile location.

[0148]

Note that the hardware configuration in FIG. 20 is one example and does not limit the scope of the present invention. For example, the camera 112, microphone 114, speaker 115, or the like may be installed outside the communication device 10. Furthermore, the communication device 10 does not necessarily have to have the camera 112, microphone 114, speaker 115, or the like.

[0149]

Furthermore, the communication device 10 may further have a control unit for implementing the car navigation function, in addition to the control unit 122 for controlling the communication device 10. Moreover, each constituent element constituting the communication device 10 may be divided into a plurality of devices and provided within the vehicle; for example, a car navigation device, communication device, or the like. Alternatively, the vehicle itself, such as vehicles 1901, 1902, or the like may be the communication device 10.

[0150]

Moreover, the communication device 10 may be a general-type navigation device or the like that does not have the vehicle speed sensor 2102 or the like.

[Description of Reference Numerals]

[0151]

2 Communication network

10, 10da, 10db Communication device

40, 40da, 40db External input device (external device)

500, 1400, 1800, 1900 Communication system

501 LAN

60a, 60b Access point

80 Communication management device

601 Wireless communication means

602 Wired communication means (communication means)

603 Display means

604 Acquisition means

605 Connection request means

608 Server means

609 Login authentication means

610 Password generation means

1201 Second wireless communication means

1801 Second wired communication means

[Citation List]

[Patent Documents]

[0152]

[Patent Literature 1] JP 2011-188312 A

[Patent Literature 2] JP 2010-218417 A

1.

A communication device, comprising:

communication means capable of one-to-one connection with an external device holding certificate information required to connect to a network;

acquisition means for acquiring the certificate information from the external device connected by the communication means; and

connection request means for sending a request for connection to the network to a communication management device, which performs authentication to determine whether to permit a connection to the network, using the certificate information acquired by the acquisition means.

2.

The communication device according to claim 1, wherein the communication means is wired communication means for connecting to the external device via a wire.

3.

The communication device according to claim 2, further comprising wireless communication means for connecting to the network wirelessly when a connection to the network is permitted by the communication management device.

4.

The communication device according to claim 2, further comprising wired communication means for connecting to the network via a wire when a connection to the network is permitted by the communication management device.

5.

The communication device according to claim 1, wherein the communication means is wireless communication means for connecting to the external device wirelessly.

6.

The communication device according to claim 4, further comprising wireless communication means for connecting to the network wirelessly when a connection to the network is permitted by the communication management device.

7.

The communication device according to any one of claims 1 to 6, wherein communication with the external device using the communication means is encrypted.

8.

The communication device according to any one of claims 1 to 7, further comprising:

display means for displaying authentication information required to login to connect to the external device using the communication means; and

login authentication means for authenticating whether the login is permitted, using the authentication information displayed by the display means; wherein

when the login authentication means permits the login, the connection request means sends a request for connection to the network to the communication management device using the certificate information.

9.

The communication device according to claim 8, wherein the authentication information contains a one-time password that is different information each time it is displayed by the display means.

10.

The communication device according to claim 8 or 9, further comprising server means for providing a web page for inputting the authentication information.

11.

The communication device according to any one of claims 1 to 10, wherein the communication means comprises primary communication means and secondary communication means; and

when a connection to the external device is performed by the primary communication means, the secondary communication means is disabled.

12.

A communication system, comprising the communication means according to any one of claims 1 to 11, and an external device; wherein

the external device comprises:

communication means capable of one-to-one connection with the communication device;

means for storing certificate information required to connect to the network; and

means for transmitting the certificate information to the communication device via the communication means capable of connecting with the communication device.

13.

A program for causing the communication device to function as:

acquisition means for acquiring certificate information from an external device connected by communication means capable of one-to-one connection with the external device holding the certificate information required to connect to a network; and

connection request means for sending a request for connection to the network to a communication management device, which performs authentication to determine whether to permit a connection to the network, using the certificate information acquired by the acquisition means.

14.

The program according to claim 13, further causing to operate as:

display means for displaying authentication information required to login to connect to the external device using the communication means;

login authentication means for authenticating whether the login is permitted, using the authentication information displayed by the display means; and

the acquisition means as means for acquiring the certificate information from the external device when the login is permitted by the login authentication means.

[Document Name] Abstract

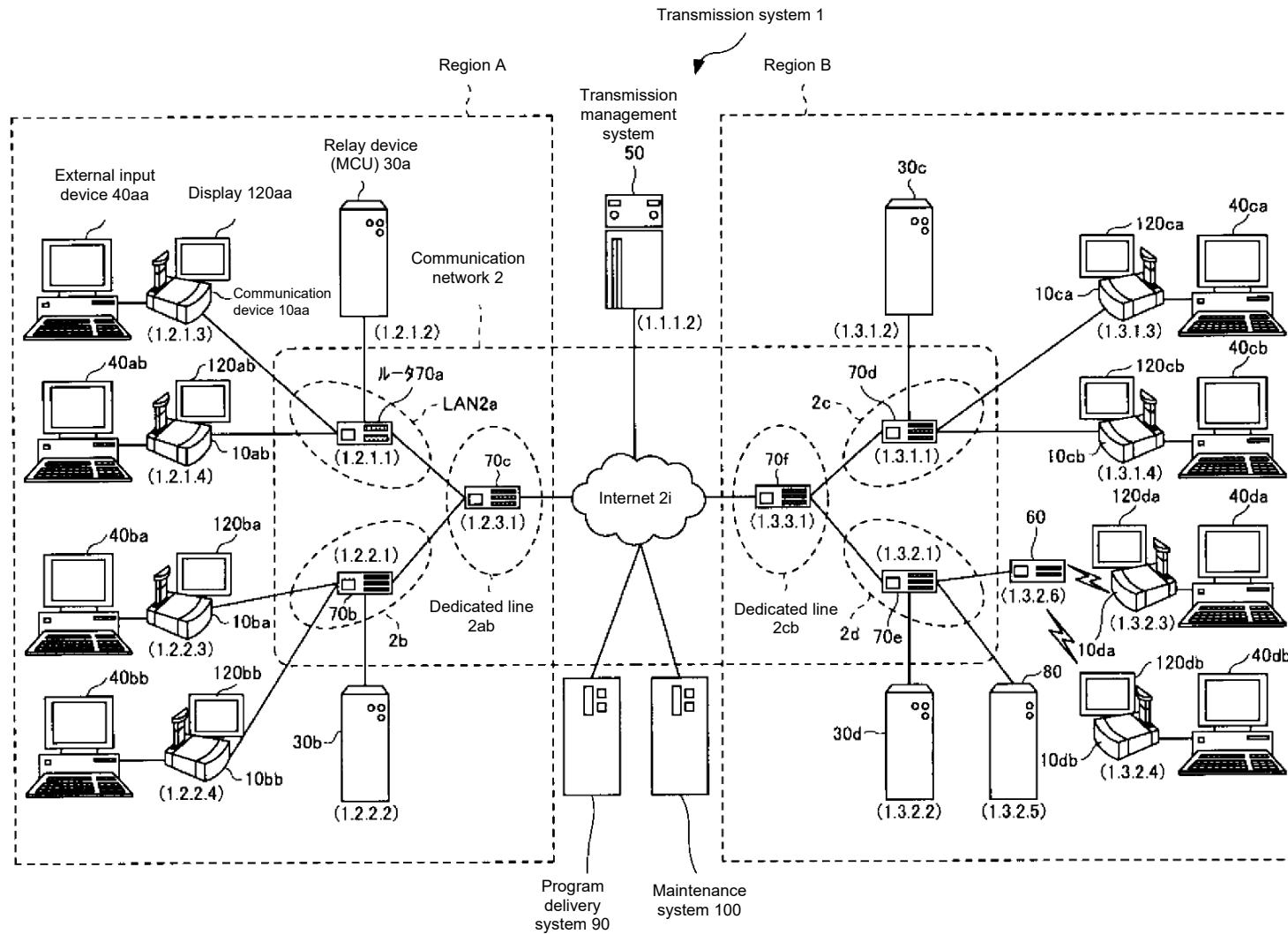
[Abstract]

[Problem] An object is to provide a communication device that enables users to easily configure security information while strengthening the prevention of leakage of information.

[Solution Means] The communication device has communication means capable of one-to-one connection with an external device holding certificate information required to connect to a network; acquisition means for acquiring the certificate information from the external device connected by the communication means; and connection request means for sending a request for connection to the network to a communication management device, which performs authentication to determine whether to permit a connection to the network, using the certificate information acquired by the acquisition means.

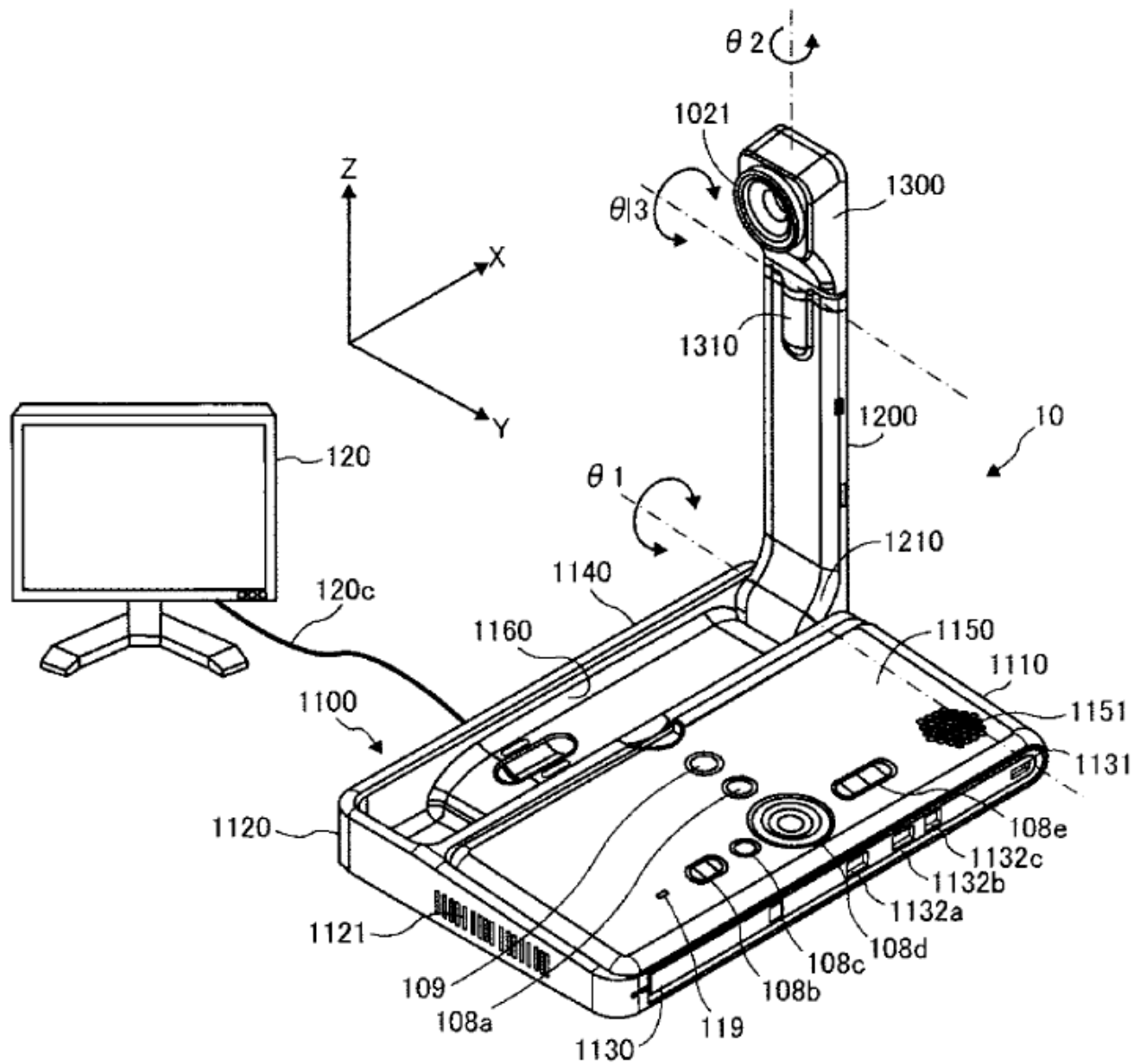
[Selected Drawing] FIG. 6

Schematic diagram of transmission system according to the first embodiment



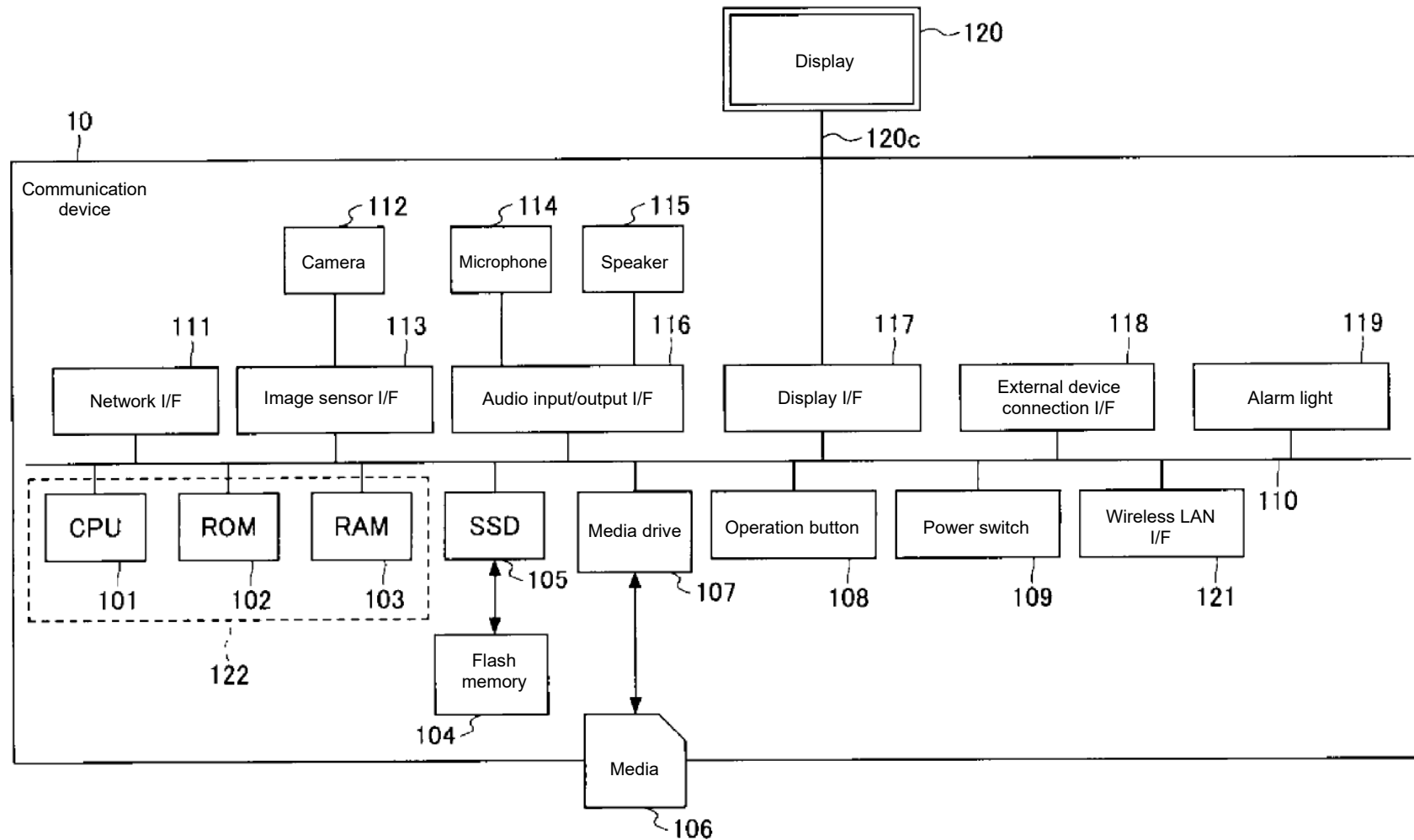
[FIG. 2]

External view of communication device according to the first embodiment



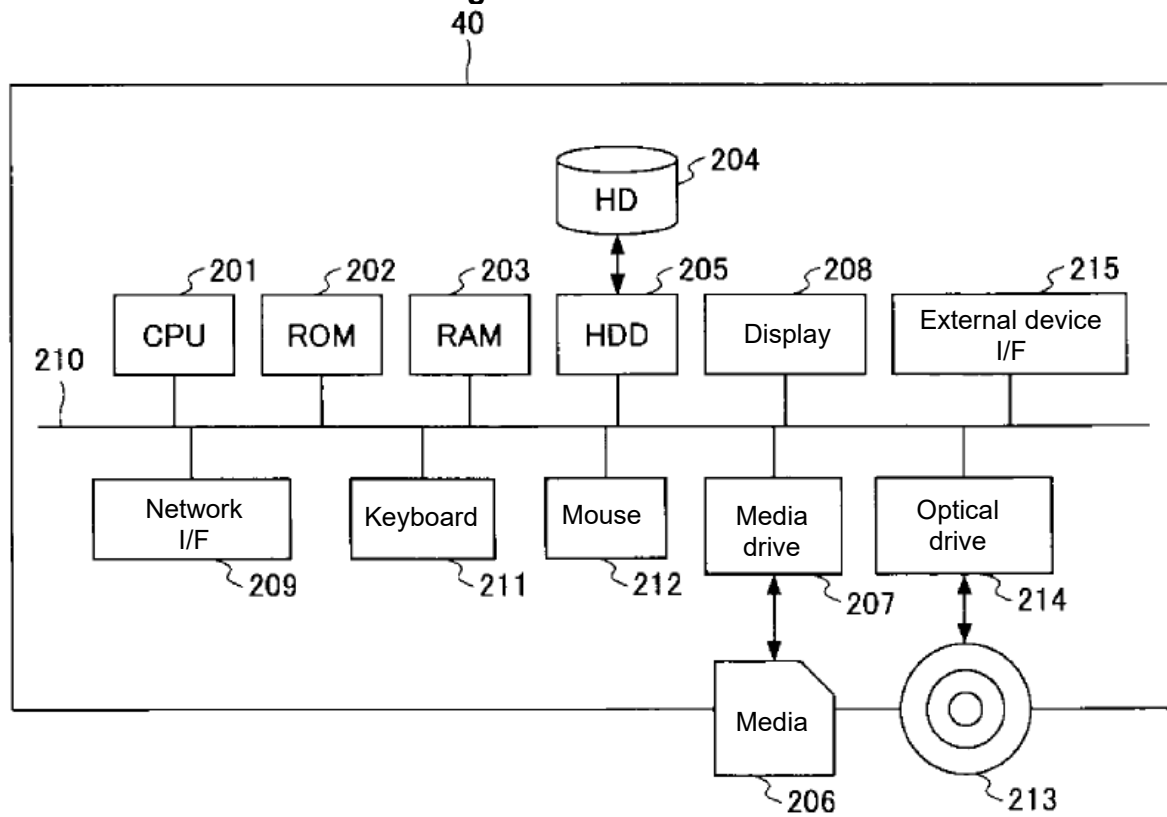
[FIG. 3]

Hardware configuration diagram of communication device according to the first embodiment

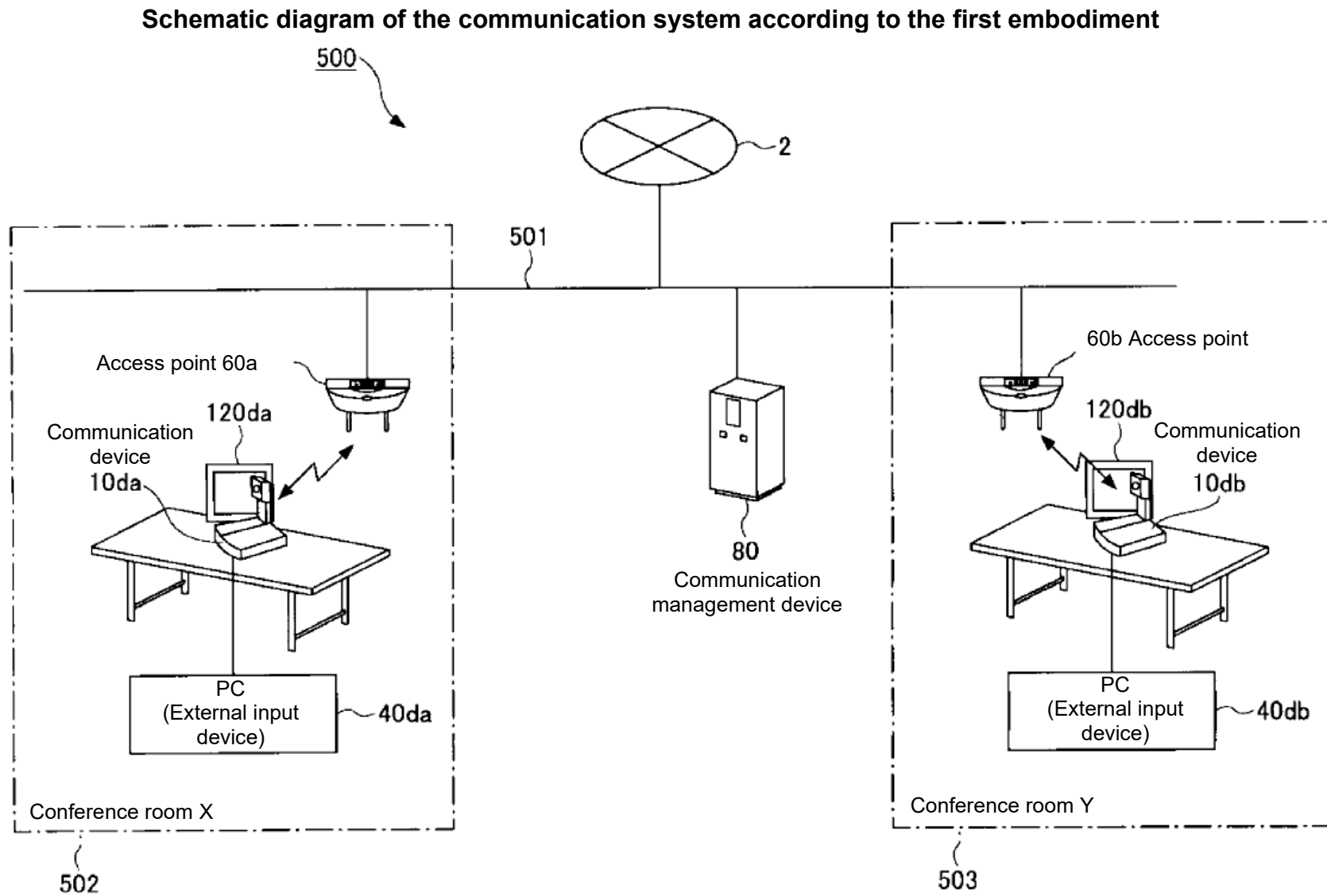


[FIG. 4]

**Hardware configuration diagram of external input device
according to the first embodiment**

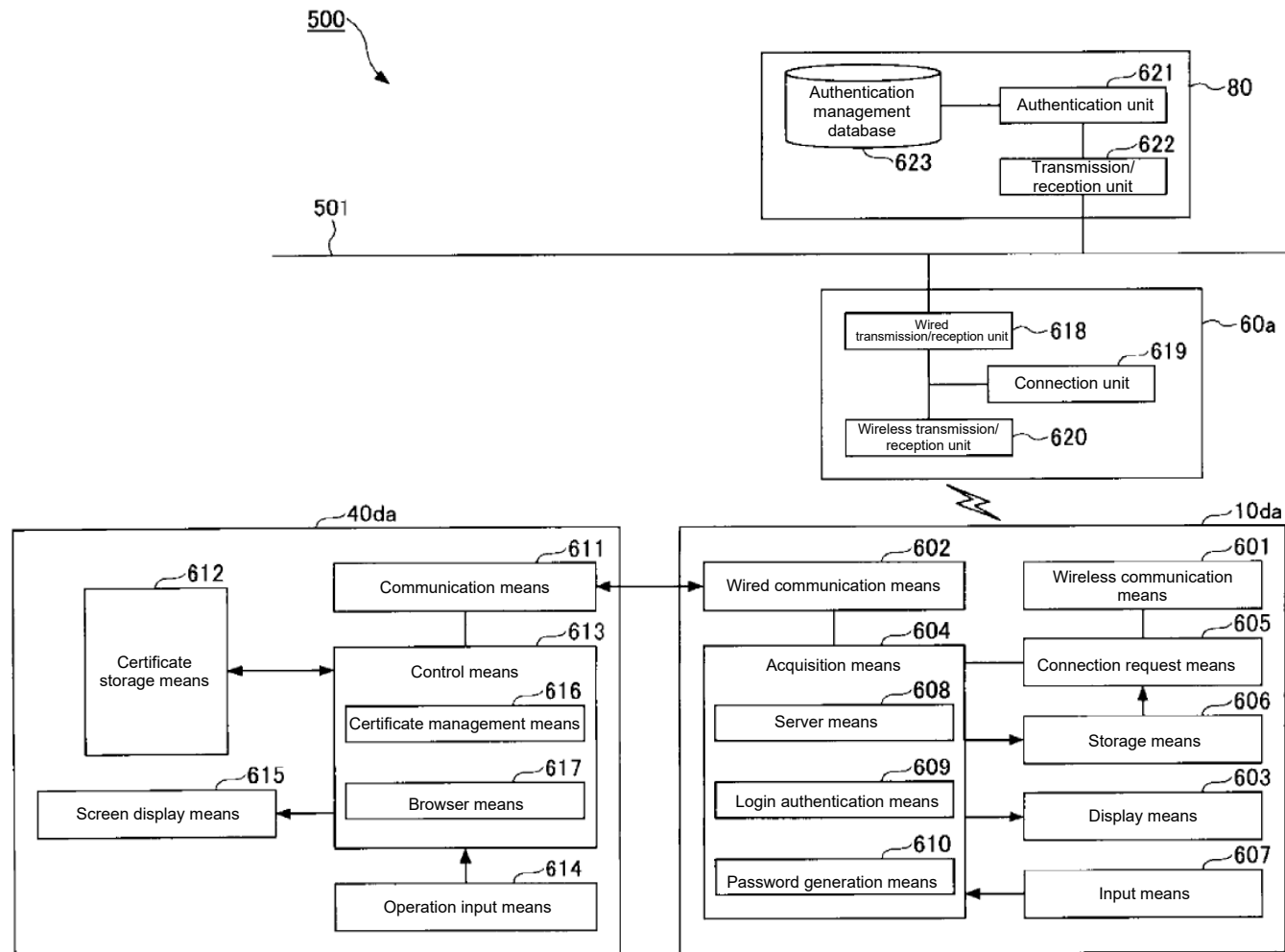


[FIG. 5]



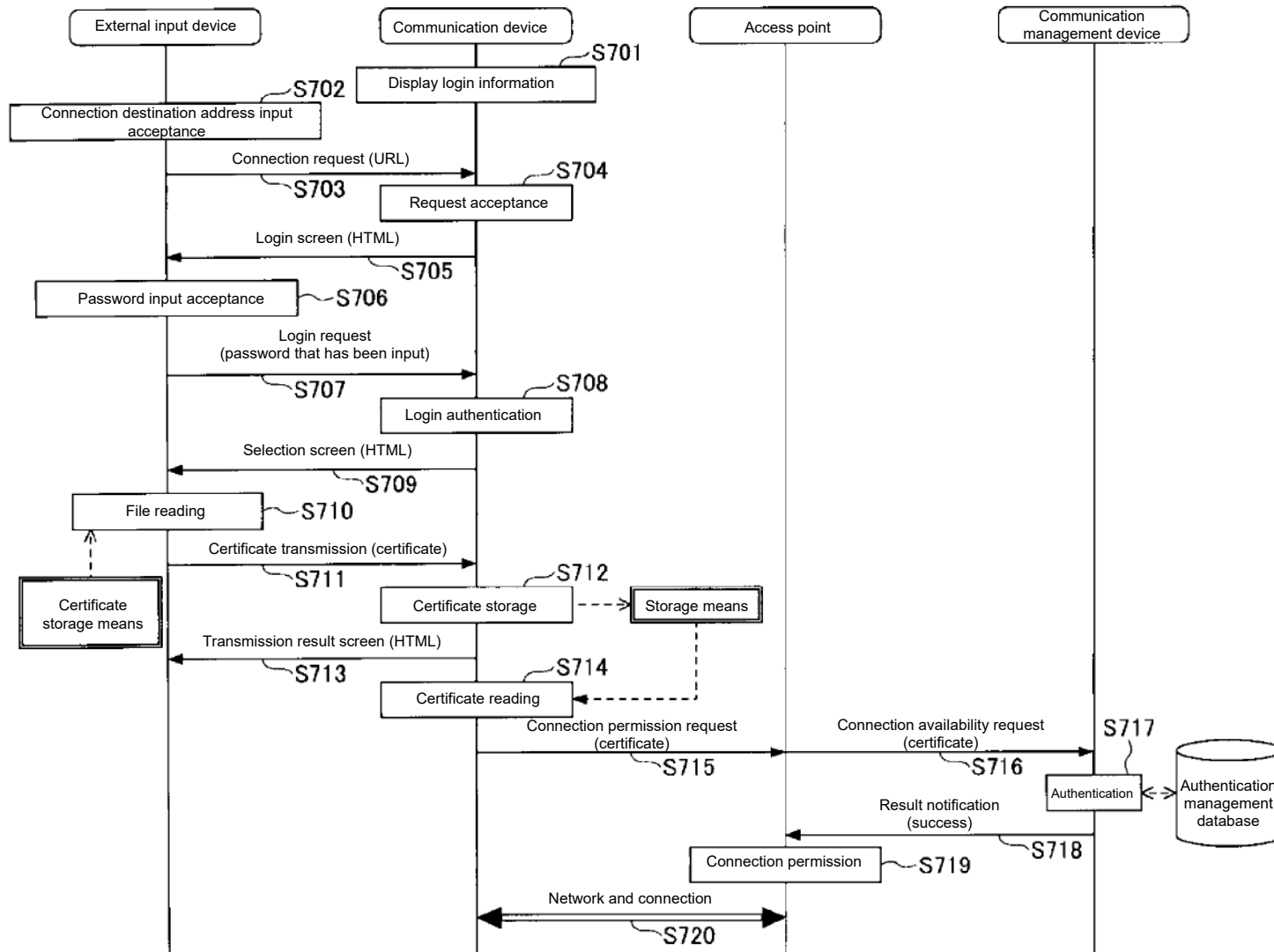
[FIG. 6]

Functional configuration diagram of the communication system according to the first embodiment



[FIG. 7]

Sequence chart illustrating the flow of processing by the communication system according to the first embodiment



[FIG. 8]

Example of display of login information according to the first embodiment

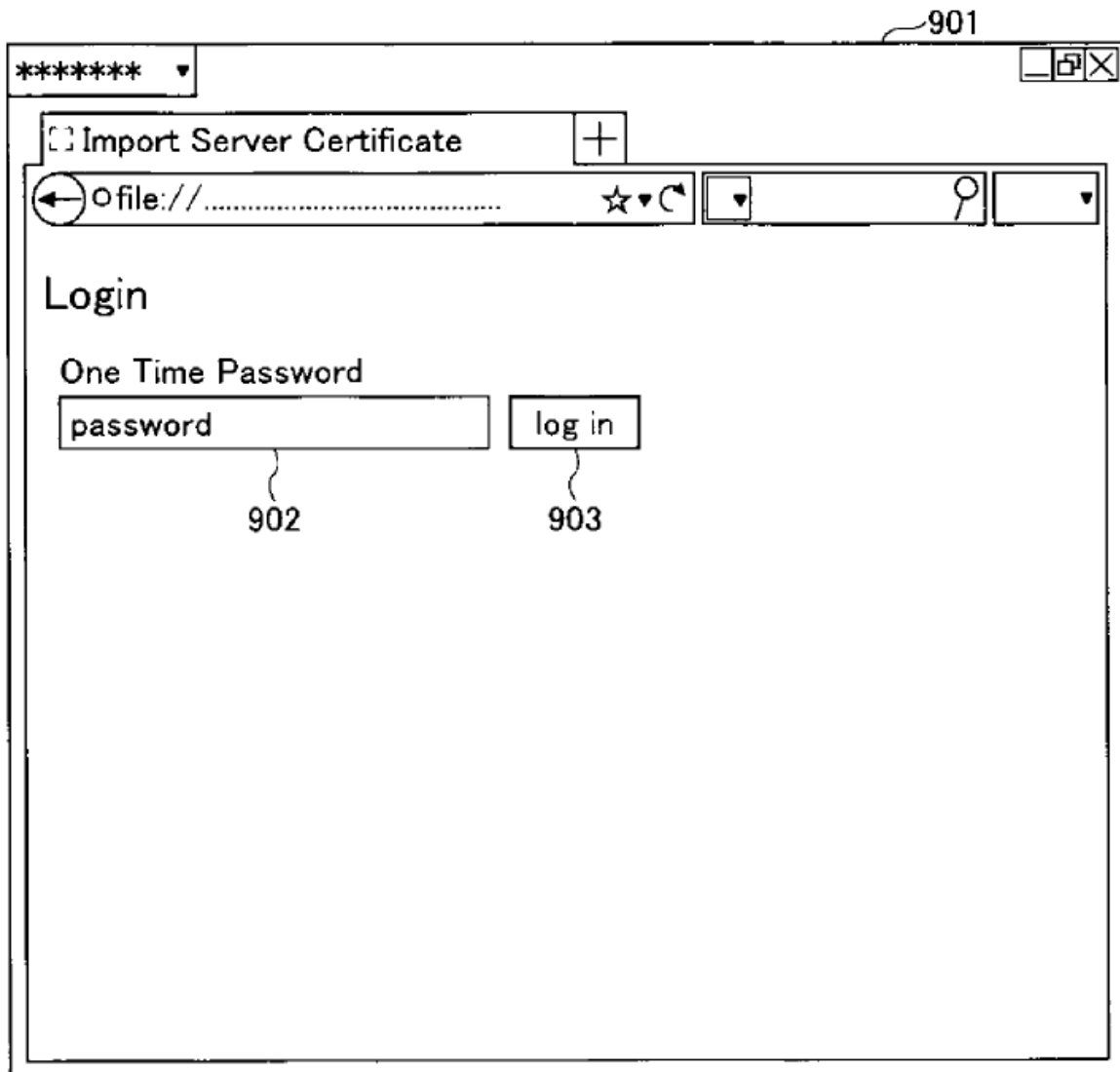
120

801 Destination address URL
https://

802 One-time password for server certificate
XXXXXX

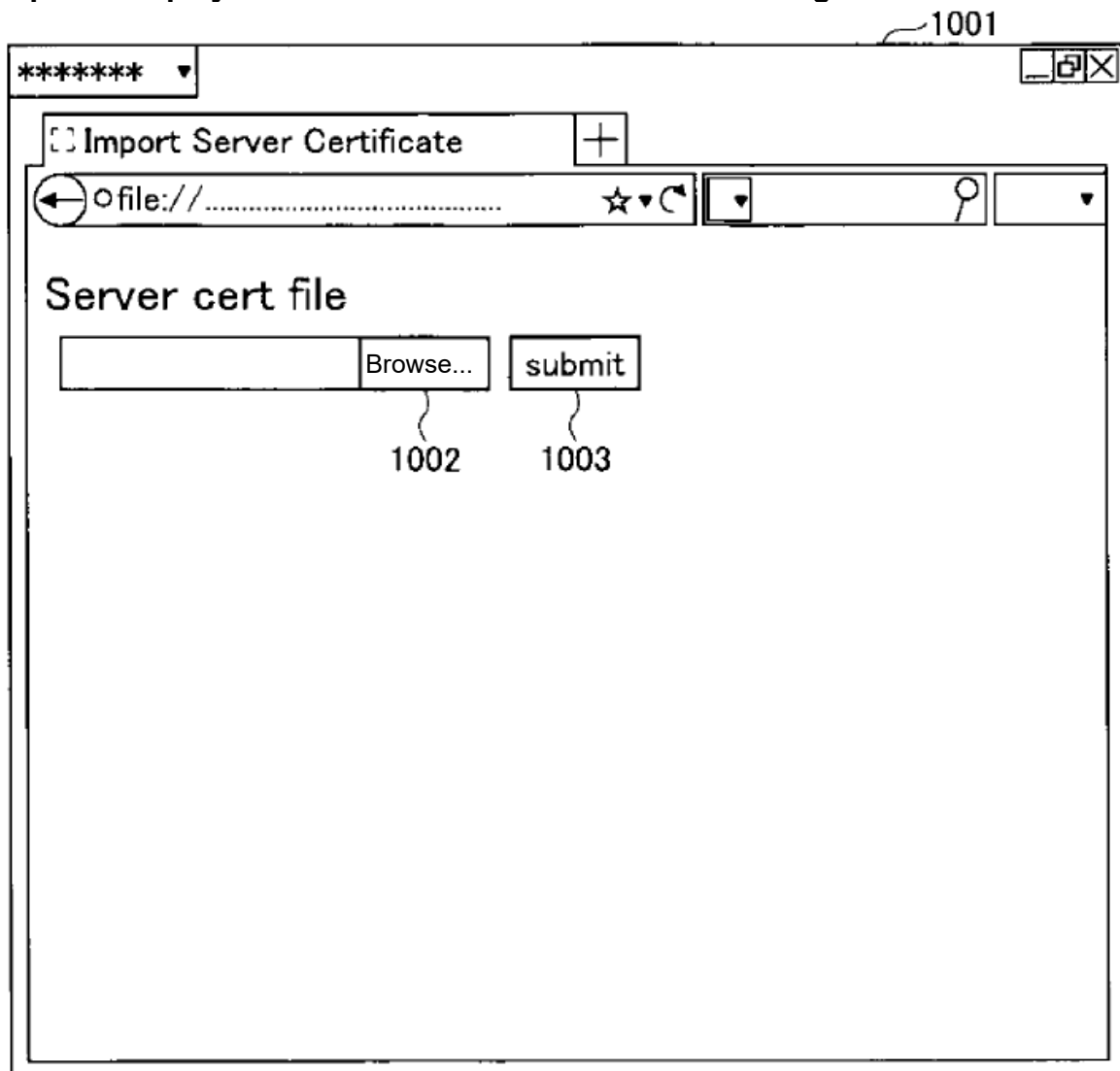
[FIG. 9]

Example of display of login screen according to the first embodiment



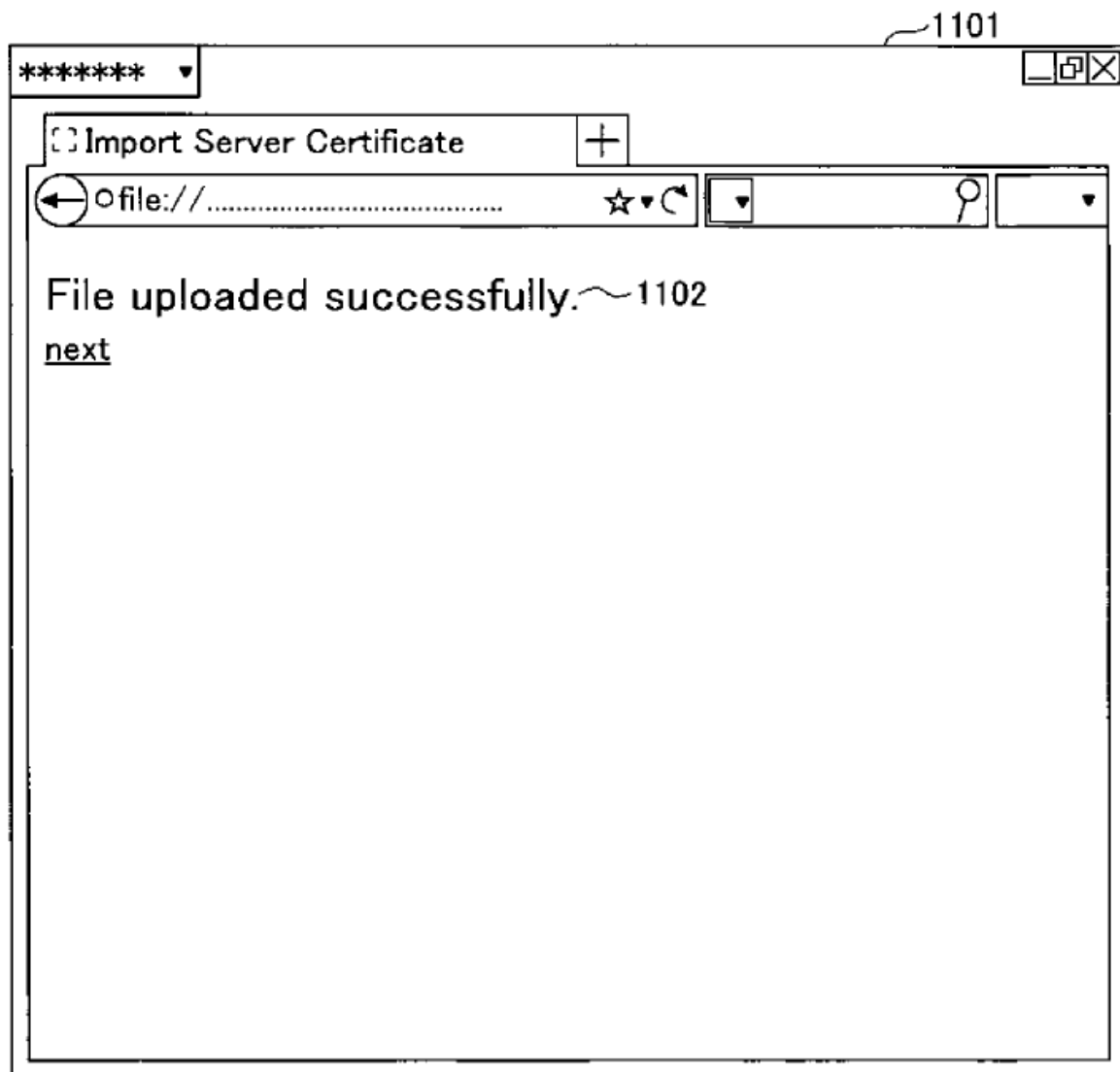
[FIG. 10]

Example of display of certificate selection screen according to the first embodiment



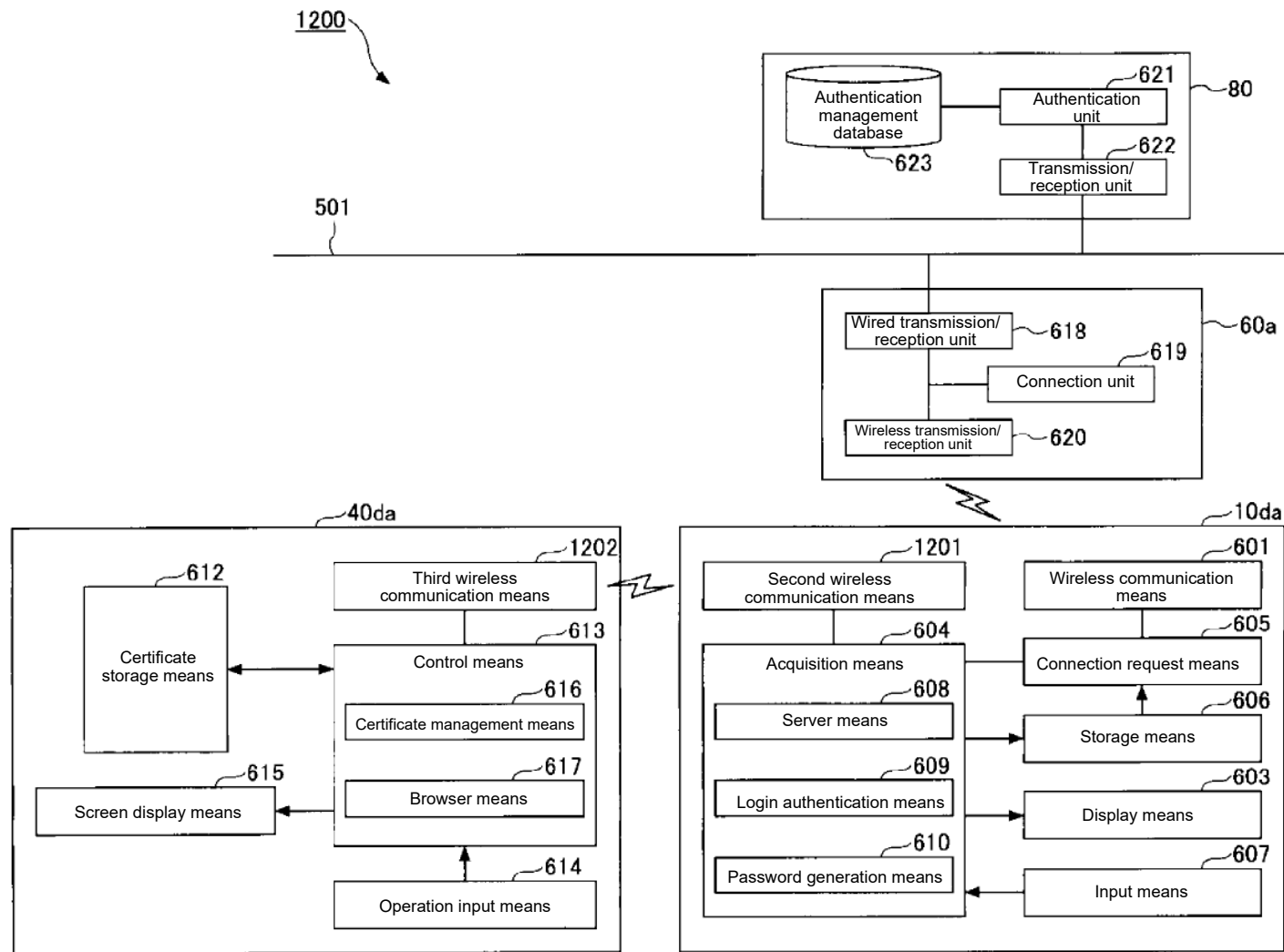
[FIG. 11]

Example of display of results display screen according to the first embodiment



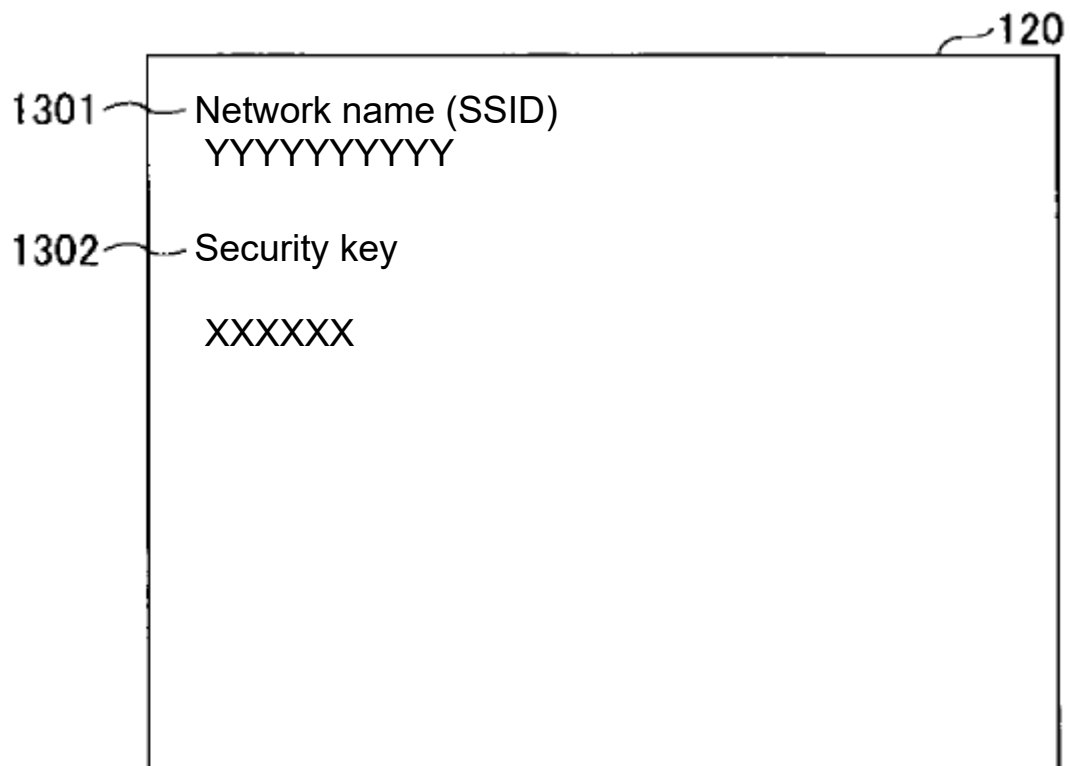
[FIG. 12]

Functional configuration diagram of the communication system according to the second embodiment



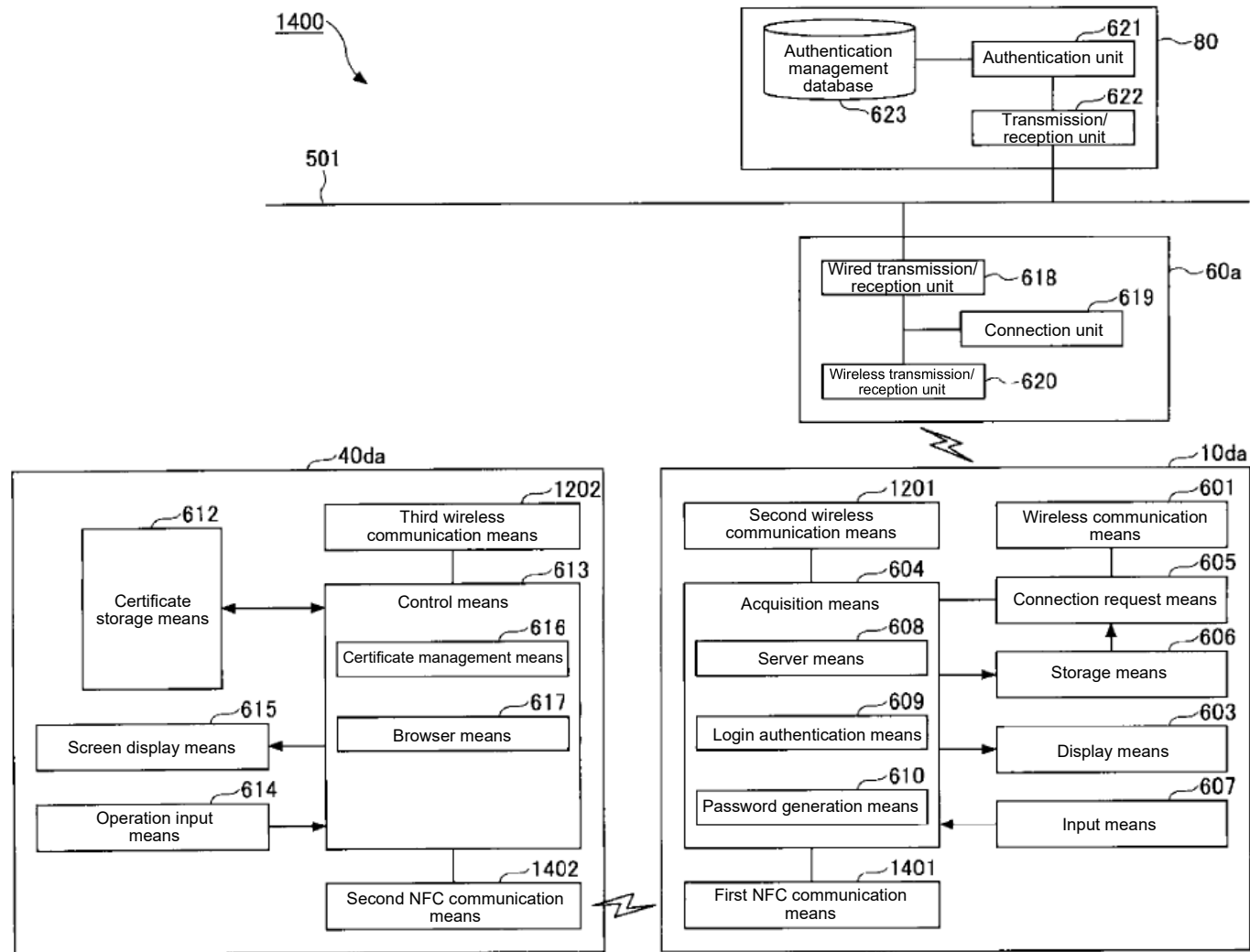
[FIG. 13]

Example of display of ad hoc mode configuration information according to the second embodiment



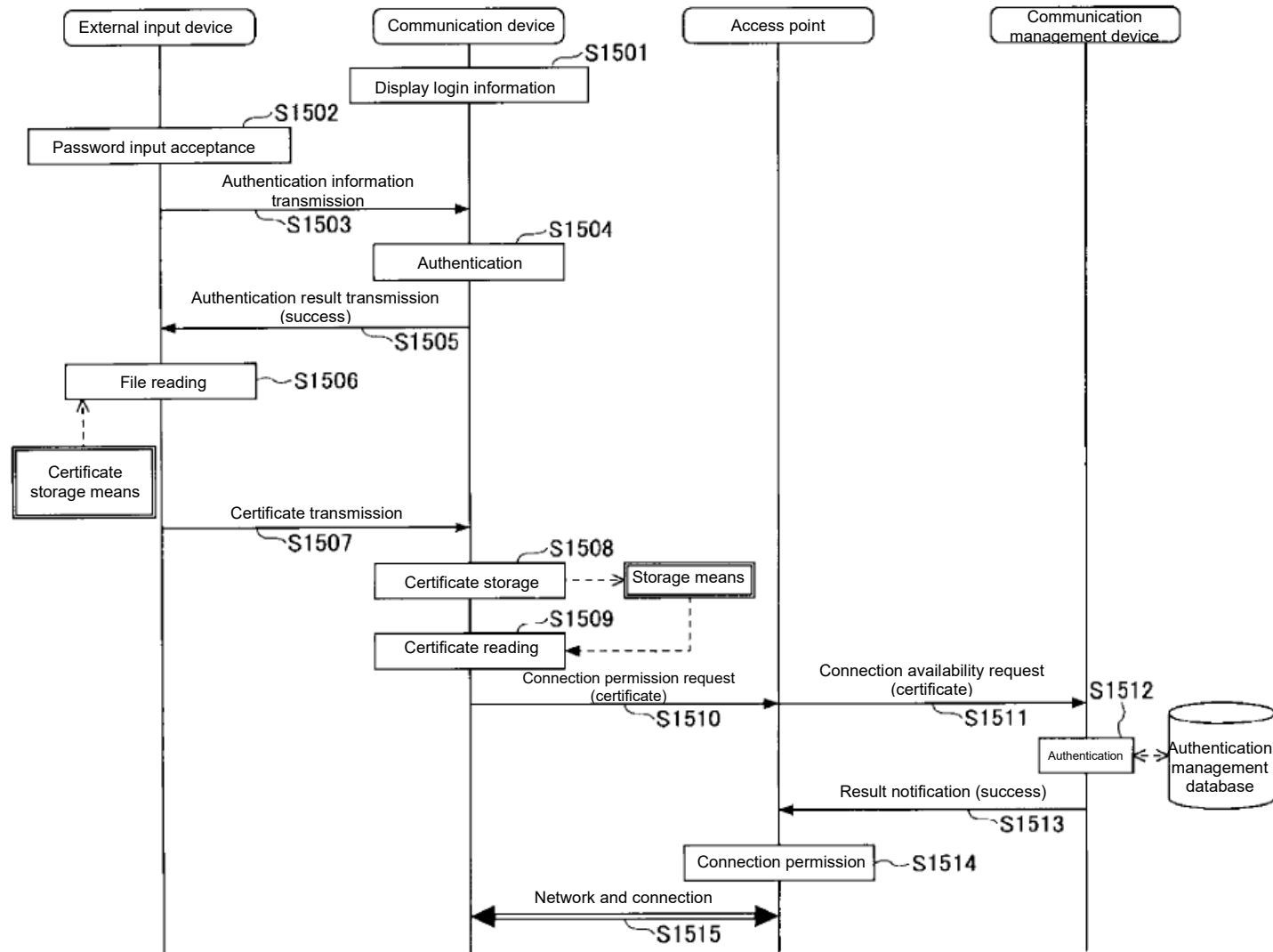
[FIG. 14]

Functional configuration diagram of the communication system according to the third embodiment



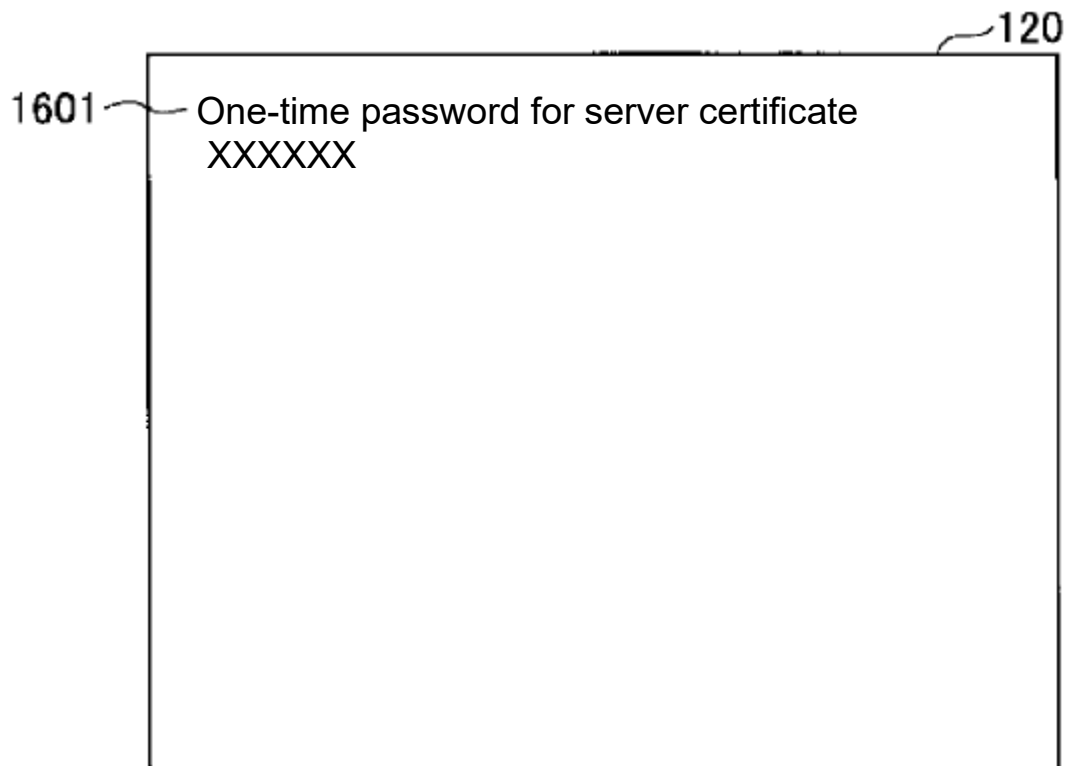
[FIG. 15]

Sequence chart illustrating the flow of processing by the communication system according to the third embodiment



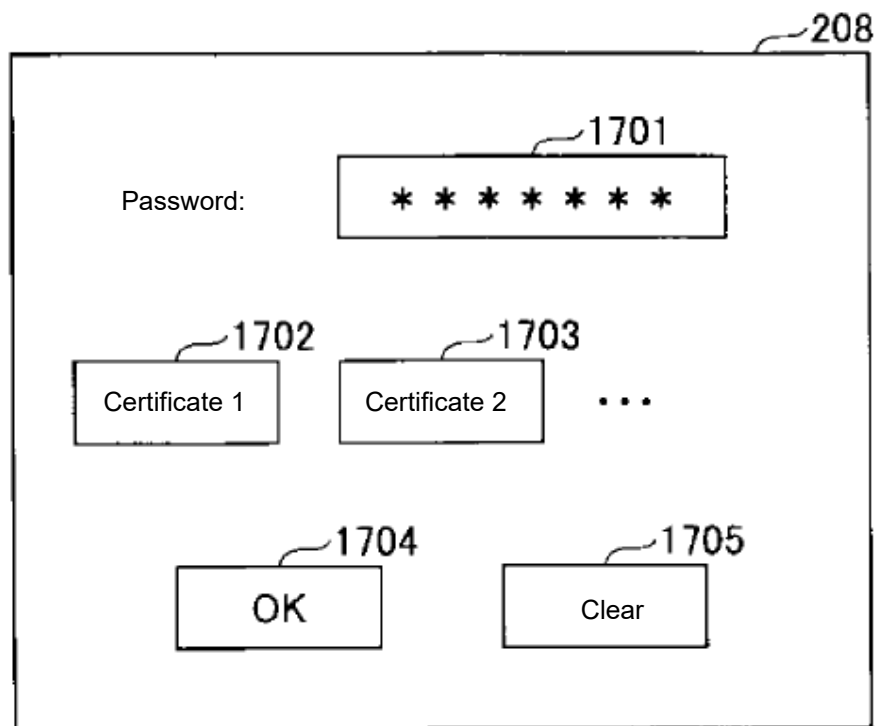
[FIG. 16]

Example of display of login information according to the third embodiment



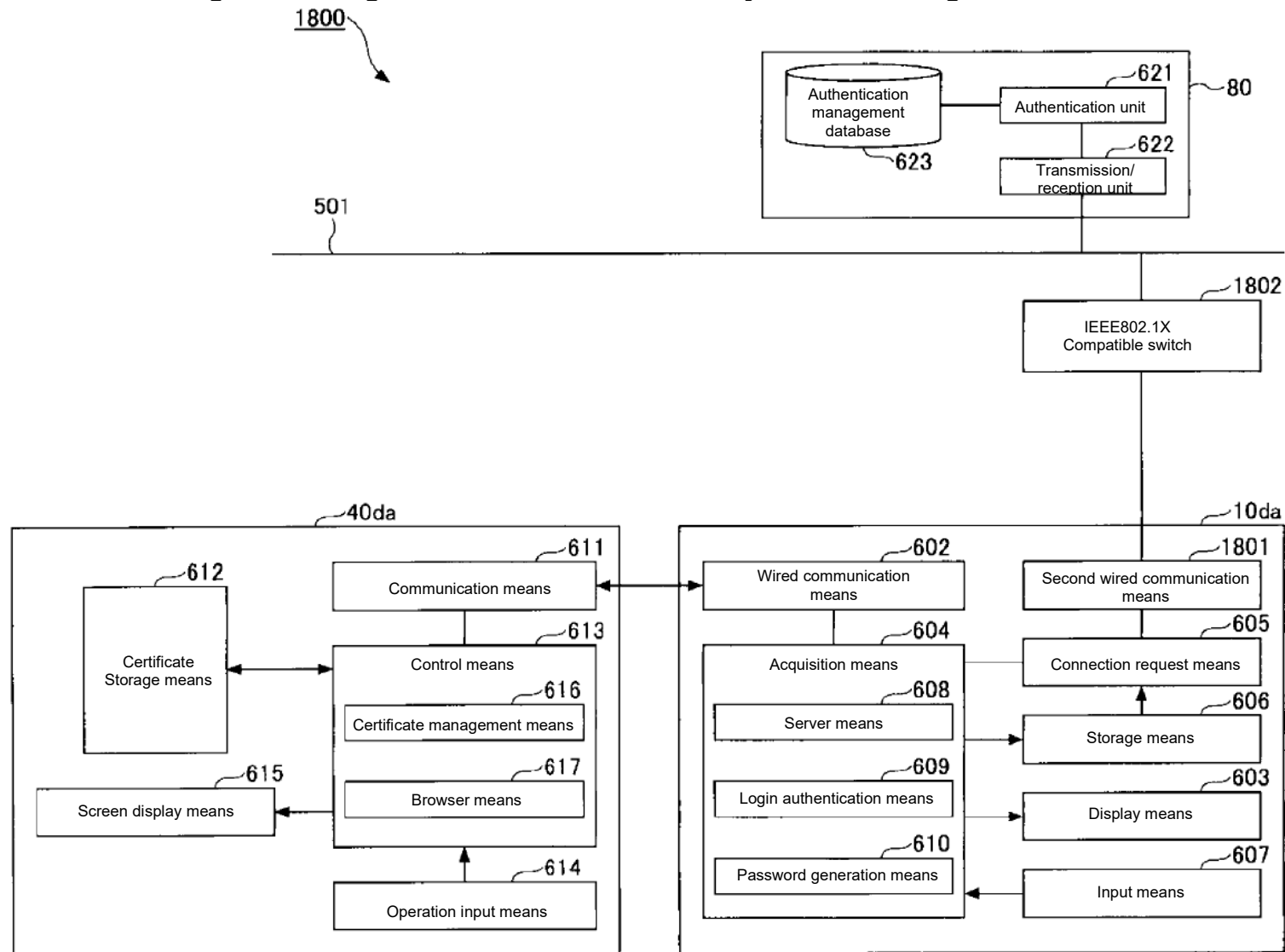
[FIG. 17]

Example of display of a one-time password input screen according to the third embodiment



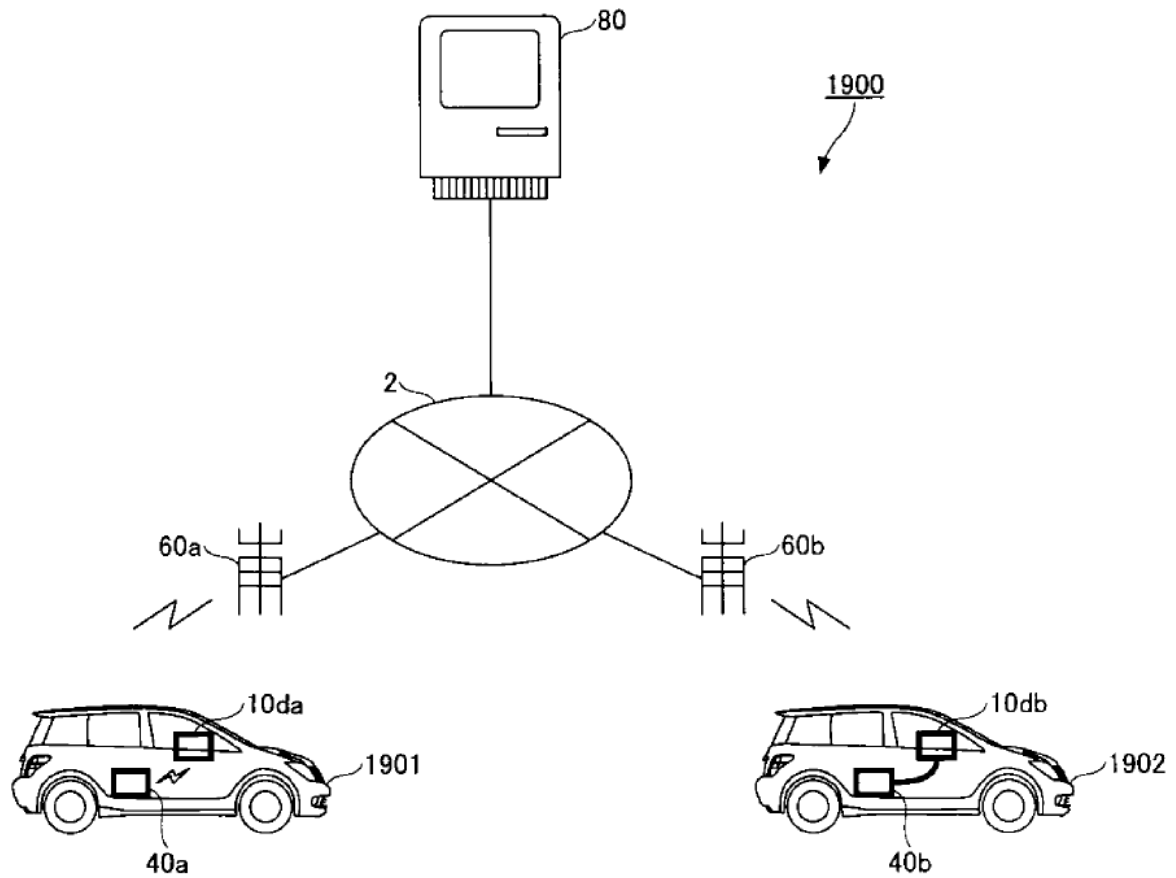
[FIG. 18]

Functional configuration diagram of the communication system according to the fourth embodiment



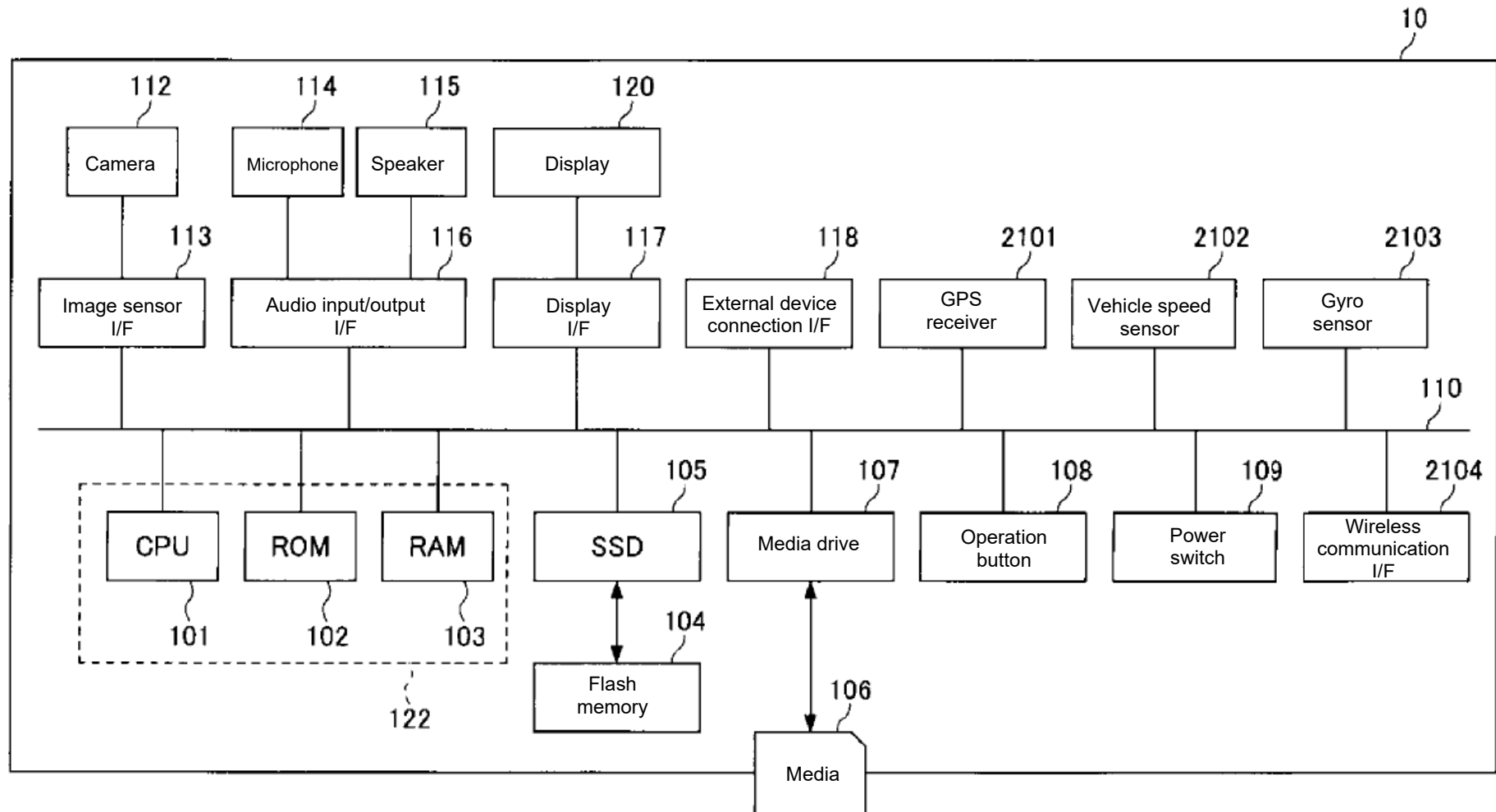
[FIG. 19]

Diagram illustrating a configuration example of the communication system according to the fifth embodiment



[FIG. 20]

Diagram illustrating a configuration example of the hardware of the communication system according to the fifth embodiment



Applicant History

000006747

20020517

Address Change

1-3-6 Nakamagome, Ota-ku, Tokyo

The Ricoh Company, Ltd.

TRANSLATION CERTIFICATION

Date: 2025/07/18

To whom it may concern:

This is to certify that the attached translation is an accurate representation of the documents received by this office. The translation was completed from:

- Japanese

To:

- English (USA)

The documents are designated as:

- 'JP2014-006624'

Samuel Wu, Managing Director of this company, attests to the following under penalty of perjury:

"To the best of my knowledge, the aforementioned documents are a true, full and accurate translation of the specified documents."



Signature of **Samuel Wu**, Managing Director



TRANSLATOR CERTIFICATION

Date: July 21, 2025

To whom it may concern:

I, [Lorelle K.], a translator fluent in the [Japanese] and [English] languages, on behalf of Morningside Translations, attest to the following under penalty of perjury:

To the best of my knowledge, the aforementioned documents are a true, full and accurate translation of the specified documents.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

The document is designated as:

- [JP2014-006624]

A handwritten signature in cursive script, appearing to read "Lorelle K.", is written above a horizontal line.

Signature

[Lorelle K.]

Print