(19) DANMARK

(10) **DK/EP 3732869 T3**

Patent- og
Varemærkestyrelsen

(12) Oversættelse af
europæisk patentskrift

(51) Int.Cl.: ***H 04 L 29/08 (2006.01)*** ***G 06 F 3/023 (2006.01)*** ***G 06 F 3/033 (2013.01)***
G 06 F 13/10 (2006.01) ***G 06 F 21/34 (2013.01)*** ***G 06 F 21/42 (2013.01)***
G 06 F 21/83 (2013.01) ***G 06 F 21/85 (2013.01)***

(45) Oversættelsen bekendtgjort den: **2021-02-01**

(80) Dato for Den Europæiske Patentmyndigheds
bekendtgørelse om meddelelse af patentet: **2021-01-06**

(86) Europæisk ansøgning nr.: **19714184.9**

(86) Europæisk indleveringsdag: **2019-03-26**

(87) Den europæiske ansøgnings publiceringsdag: **2020-11-04**

(86) International ansøgning nr.: **EP2019057558**

(87) Internationalt publikationsnr.: **WO2019211045**

(30) Prioritet: **2018-05-04 DK PA201870268**

(84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **BifrostConnect ApS, Njalsgade 76, 2300 København S, Danmark**

(72) Opfinder: **STANFELD, Benjamin, Langøgade 23, 3 th., 2100 København Ø, Danmark**

(74) Fuldmægtig i Danmark: **Inspicos P/S, Kogle Alle 2, 2970 Hørsholm, Danmark**

(54) Benævnelse: **A remote support device**

(56) Fremdragne publikationer:
WO-A1-2013/023195
US-A1- 2007 113 267

DESCRIPTION

FIELD OF THE INVENTION

[0001] The present invention relates to a portable remote support device and a method for remote supporting computer equipment.

BACKGROUND OF THE INVENTION

[0002] Most computer equipment, such as Personal Computers (PCs), servers, routers, switches, IoT devices, robots, household appliances, etc., will at some point during its lifetime require support for, e.g., setup, connection and hardware failures, malfunction, software updates, restarts after a power loss, or the like.

[0003] Computer equipment, such as servers and/or PCs, often contains information which is critical to operations, and the physical and virtual access to them is therefore often restricted. Virtual access is often restricted by layers of antivirus/anti-spyware/anti-malware software, secure network setups, and security policies preventing virtual and/or physical access to the computer equipment by prohibiting unknown hardware, such as USB-devices, to be connected to the servers. Furthermore, network problems may occur with respect to a communication network which the equipment is connected to. Similarly, physical access is typically restricted e.g. by the server room being securely locked with only a few IT-competent, trusted employees being granted access. These trusted employees have a basic understanding of computer equipment, but may not have the necessary skillset to handle more complex situations.

[0004] Thus, a specialised technician is typically required to set up and support the computer equipment. In order to do so, the specialised technician will typically need access to an input device, such as a mouse and/or a keyboard, as well as a display showing e.g. the screen output of a PC/server. The specialised technician might additionally or instead need a supporting device, such as a smartphone, a tablet computer, or a PC, to communicate with and/or sending commands to the computer equipment over e.g. a serial connection. Hence, the input devices, display and/or the supporting device will need to be connected to the computer equipment.

[0005] A need for higher efficiency and reduced downtime has made "remote access" solutions increasingly popular in recent years. However, existing solutions have some critical limitations as they need 1) Internet connection or 2) "fully working computer". Downtime is often caused by these two factors, resulting in a need of a physical presence by a specialised technician.

[0006] The support of computer equipment, therefore, typically requires a specialised technician to be physically present whilst supporting the computer equipment. Thus, a

specialised technician may either be located on-site or travel to the equipment every time support is needed.

[0007] Many companies have centralised specialised technicians, and having them travel to various locations will be very expensive and the response time will be too long. Reducing downtime is critical as a company may be completely or partially prohibited from operations, thus leading to high costs for the companies including losses in goodwill and reputation.

[0008] US 8,595,321 discloses a remote control support system providing a simple way to allow remote users to access a computer in a variety of circumstances, even when no software is installed on the computer. In some cases, the system includes a hardware device to simulate most USB mice, keyboards, storage devices, camera sensors (to capture a screen display), etc. The hardware device can communicate with a remote computer (via a network connection) to allow a user, such as a remote technician, to work on the remote computer as if the user was sitting at the remote computer. Information technology professionals and other users can use the described systems to communicate with a user at a remote computer in a natural way to communicate via voice, video or chat with online messaging.

[0009] Thereby, a technician may be located remotely and through a network connection connect a supporting device, i.e. a remote computer, to a remote support device, which is powered and connected to a piece of computer equipment to be supported. Through this network connection, the technician can send, e.g., mouse commands, keystrokes or other communication to the piece of computer equipment to be supported.

[0010] This, however, requires the remote support device to be set up in place and powered, before the technician can connect to the remote support device. Thus, the remote support device must be installed permanently, which allows a remote support device to support only one piece of computer equipment. Consequently, this may require a large initial installation time of the remote support device as well as high costs by having one remote support device per computer equipment.

[0011] Alternatively, the remote support device may be moved and connected to another piece of computer equipment by a trusted person by disconnecting, moving and reconnecting the remote support device to the other piece of computer equipment. The technician will then have to reconnect to the remote support device upon every movement of the computer equipment. Moreover, in an environment, e.g. a server room, with power outages, the technician will lose the connection to the remote support device and needs to reconnect with every power loss. Furthermore, the technician may have to remain in contact with the trusted person during the movement of the remote support device, e.g. over the phone, to provide information regarding whether the device has been connected correctly or not.

[0012] WO 2013/023195 discloses a network device and a method for remote computer operation. The network device comprises a processor, an interface for emulating a human interface device, a video input, and a data storage for storing data from a target device or

transferring data to the target device. The network device further comprises a first network interface, and is configured to provide control of a target device, through the interface for emulating a human interface device.

[0013] US 2007/113267 discloses a portable device enabling access to a host computer via a guest computer. The portable device is connected to the guest computer, and a program stored in a memory on the portable device is activated, the program including instructions for establishing communication with the host computer such that input to the guest computer serves as input to the host computer, and output displays from the host computer are displayed on the guest computer.

DESCRIPTION OF THE INVENTION

[0014] The invention relates to a portable remote support device, as further defined in claim 1, and a method, as further defined in claim 8, for remote supporting computer equipment.

[0015] It is an object of embodiments of the invention to provide a remote support method and a device for remote support of computer equipment, which is more time-efficient and has a higher connection stability in use.

[0016] It is a further object of embodiments of the invention to provide a remote support method and a device for remote support of computer equipment, in which the risk of third parties gaining unauthorised access to the computer equipment through the remote support system is minimised.

[0017] It is an even further object of embodiments of the invention to provide a remote support method and a device for remote support of computer equipment which is easy to use without compromising security.

[0018] It is an even further object of embodiments of the invention to provide a remote support method and device for remote support of computer equipment, in which remote access is available, even if the network is down.

[0019] According to a first aspect the invention provides a portable remote support device comprising a processing unit, a network communication unit configured to communicate with a cloud service, a video capturing unit, at least one video input port and at least one output port, said processing unit being configured to communicate video signals received via the video input port to the cloud service via the network communication unit, and said processing unit being configured to emulate pointing device signals and/or keyboard signals received via the network communication unit on said at least one output port, and wherein the portable remote support device is configured to obtain unique secure tokens.

[0020] Here, the pointing device signal may be a mouse signal, a trackball signal, a touchpad

signal, a trackpoint signal, a joystick signal, a touch screen input signal, or any combination thereof. Additionally, the keyboard signal may be a signal from a QWERTY-keyboard or national variants thereof, a T9-style keyboard, a numeric keypad, a MIDI-keyboard, an emulator of any of these, or any combination thereof. The portable remote support device may, e.g., comprise a first and a second output port, in which case pointing device signals may be emulated on the first output port and keyboard signals may be emulated on the second output port.

[0021] The at least one output port may furthermore be a serial port using a serial communication, such as Recommended Standard 232 (RS-232), Universal Asynchronous Receiver-Transmitter (UART), Universal Synchronous and Asynchronous Receiver-Transmitter (USART), or preferably the Personal System/2-specification (PS/2), or any combination thereof. As e.g. server environments are typically subject to strong security policies, connecting external devices via e.g. a USB-connection, through which software may be transmitted, is not preferred, and may be considered a breach of security. The at least one output port may, thus, use a standard protocol only allowing an e.g. mouse and/or keyboard input, such as the PS/2 and IBM Standard Protocol. Thereby, the remote support device provides an additional security, as malicious software, such as a computer virus, malware, or spyware, may not be able to be transmitted through the at least one output port, in case unauthorised access to, such as hacking of, the portable support device occurs.

[0022] The remote support may be unattended by a trusted person, as the technician can control the computer equipment through the connected portable remote support device. Additionally, the trusted person may not need IT-competence to connect and set up the remote support device and may thus be a lay person and/or any employee of a company.

[0023] In the present context the term 'portable remote support device' should be interpreted to mean a hardware device which can easily be moved from one position to another, and which is capable of establishing support access to a piece of computer equipment from a remote location, such as a remote support centre.

[0024] In the present context the term 'computer equipment' should be interpreted to mean any kind of equipment which includes a processor, and which may be in need of remote support. Thus, the computer equipment may be in the form of personal computers (PCs), servers, routers, switches, IoT devices, robots, household appliances, sensors, etc.

[0025] The portable remote support device comprises a network communication unit configured to communicate with a cloud service. In the present context the term 'cloud service' should be interpreted to mean a service which is accessible via a network connection, such as an Internet connection, and which provides services, e.g. in the form of data storage, support, etc., on demand without direct management by the user. Thus, the network communication unit is capable of establishing a network connection between the portable remote support device and such a cloud service.

[0026] The portable remote support device further comprises a video capturing unit and at least one video input port, and the processing unit is configured to communicate video signals received via the video input port to the cloud service via the network communication unit. Thus, a video signal can be supplied from the location of the computer equipment requiring remote support to the cloud service by the portable remote support device, via the video input port and the network communication unit. The video signals may, e.g., be in the form of a video signal from a camera directed towards the computer equipment and/or in the form of a video output from the computer equipment, such as a signal which would normally be supplied to a monitor of the computer equipment. In the latter case a video signal reflecting what is normally displayed to an operator at the computer equipment via a monitor is provided to the cloud service, thereby allowing support personnel accessing the cloud service to view exactly what a locally positioned operator would view.

[0027] Furthermore, the processing unit is configured to emulate pointing device signals and/or keyboard signals, as defined above, received via the network communication unit on the at least one output port. Thereby remotely located support personnel is able to provide suitable pointing device signals and/or keyboard signals to the computer equipment requiring remote support, via the cloud service and the portable remote support device. Accordingly, the remotely located support personnel can control the computer equipment in the same manner as a locally located operator.

[0028] The portable remote support device is configured to obtain unique secure tokens. In the present context the term 'unique secure token' should be interpreted to mean unique code associated with and identifying the remote portable support device, and which needs to be applied in order to gain access to the portable remote support device. The unique secure token could, e.g., be in the form of a number with a predetermined number of digits. The unique secure token may be generated once, e.g. upon initiating use of the portable remote support device. However, the unique secure token will normally be refreshed from time to time, e.g. at predefined time intervals or in response to certain events, such as each time the portable remote support device is powered on or each time a remote support session is initiated. This will be described in further detail below. Furthermore, the unique secure token may be obtained by the portable remote support device generating the unique secure token itself, or by the unique secure token being provided to the portable remote support device from an external source, e.g. via the cloud service. This will also be described in further detail below.

[0029] Since the portable remote support device is configured to obtain unique secure tokens, it can be ensured that the communication taking place between the portable remote support device and the cloud service takes place in a secure manner, and the risk of unauthorised access to the computer equipment requiring remote support, via the portable remote support device is minimised. Furthermore, the secure communication with the remote support personnel is established in an easy manner.

[0030] Thus, the connection between at least the portable remote support device and the cloud service, and preferably also connection between the cloud service and device operated

by a technician, may be a secure connection, e.g. via HTTPS.

[0031] The portable remote support device preferably also comprises a hardware or software script blocker preventing automated scripts from causing a series of pointing device signals and/or keyboard signals on the at least one output port. The script blocker may be implemented in the processing unit and/or the network communication unit. This may increase the security of the remote support device, as any pointing device signal, such as a cursor movement, and/or any keyboard signal, such as entering a character, on the computer equipment will be visible on the display and, thus, also visible to the technician and/or the trusted person. The technician and/or the trusted person may abort the support session and/or disconnect the device if e.g. undesired characters and/or cursor movements occur on the computer equipment. Hence, a potential hacker may be prevented from causing unwanted actions on the piece of computer equipment to be supported.

[0032] Alternately or additionally the cloud service could be enabled to detect programming code entered via keyboard or mouse and possibly terminate connections, record such codes or alert other operators.

[0033] For additional protection, a password can be assigned to the remote support device. In this case a malicious party would need to know the secure token ID as well as the password in order to access the remote support device.

[0034] The remote support device may furthermore be used to support computer equipment outside restricted areas, e.g. in offices, home offices, or the like.

[0035] The portable remote support device may further comprise a secure token generating unit. According to this embodiment, at least some of the unique secure tokens are generated by the portable remote support device. Once a given unique secure token has been generated, the unique secure token may be shared with the cloud service, e.g. by the portable remote support device communicating the unique secure token directly to the cloud service.

[0036] Alternatively or additionally, the portable remote support device may be configured to receive secure tokens from a cloud service via the network communication unit. According to this embodiment, at least some of the unique secure tokens are not generated by the portable remote support device, but are instead provided to the portable remote support device from an external source via the cloud service. For instance, the unique secure tokens may be generated by the cloud service and subsequently shared with the portable remote support device. As an alternative, the cloud service may receive the unique secure tokens from another source and forward them to the portable remote support device.

[0037] In an embodiment, the portable remote support device comprises a display adapted to display a status of the portable remote support device. The status displayed at the display may, e.g., comprise network connection information. In the case that the portable remote support device comprises a battery, the displayed status information may comprise battery charge

information, such as state of charge (SoC).

[0038] Consequently, the trusted person or technician who e.g. sets up the remote support device may be provided with information about the system. By the status comprising network information, the trusted person, who e.g. sets this up, is able to see whether the device is connected to a network and thus connectable by a technician. As coverage of wireless connections, such as 2.4 GHz and 5 GHz wireless networks, 3G/4G/LTE, satellite networks, or the like, within a room may vary, a status showing network information may allow the trusted person to place the remote support device, where good wireless coverage is provided. Hence, latency and a percentage of lost packages may be minimised, thereby allowing for a seamless data transfer. By the display, alternatively or in combination with the network information status, being adapted to display battery charge information, such as SoC, the trusted person may estimate the remaining running time on battery and/or plan charging of the device. Furthermore, the display may show battery health, such as State of Health (SoH), which allows the trusted person to plan battery replacements with time.

[0039] The display may further be adapted to display one or more of: number of connected remote computers, mouse pointing device connection information, video connection information, and/or keyboard connection information.

[0040] Thereby, setting up, connecting, disconnecting, and/or checking a status of the remote support device may be intuitive for the trusted person, who may thus be a lay person. Similarly, the setup, connecting/disconnecting and/or checking a status may require less time for the trusted person than if he/she would have to get feedback, e.g. over the phone, from a technician who is connected to the device. Additionally, the remote support device may be set up, connected, and/or disconnected regardless of whether a technician is available at that time to connect to the remote support device.

[0041] The display may further be adapted to display unique secure tokens. According to this embodiment, the currently valid unique secure token is displayed on the display, thereby allowing the trusted person to view the token. When requesting assistance, e.g. by calling, or otherwise contacting, a technician, the trusted person can communicate the token to the technician, thereby allowing the technician to access the portable remote support device via the cloud service. This is in particular an advantage in the case that a new unique secure token is generated relatively often.

[0042] As an alternative, the unique secure token may not be displayed on the display. For instance, it may be possible to configure the display in such a manner that the token is not displayed. This could, e.g., be relevant in the case that a unique secure token is only generated once, or at very long time intervals, in which case displaying the unique secure token might lead to a security breach.

[0043] The portable remote support device may further comprising a battery adapted for powering the remote support device in use for a predetermined duration.

[0044] By the portable remote support device comprising a battery adapted for powering the remote support device in use for a predetermined duration, the remote support device may remain powered when the remote support device is not connected to an external power supply. Thereby, the remote computer of a technician may remain connected to the remote support device, whilst the device is being connected to or disconnected from a piece of computer equipment. It may, hence, be moved from one piece of computer equipment to another, whilst remaining powered, thus saving time, as several pieces of computer equipment may be supported consecutively, when the trusted person is near the computer equipment, e.g. in the server room or another access-restricted area. By the remote computer remaining connected to the remote support device, the necessary time for remote supporting several pieces of computer equipment is reduced, as reestablishment of connection between the remote computer and the remote support device may be avoided.

[0045] The predetermined duration may be sufficiently long to allow for a trusted person to disconnect the remote support device from a first piece of computer equipment, move the remote support device, and reconnect it to a second piece of computer equipment. The predetermined duration may thus be e.g. 10 minutes or less. The predetermined duration, however, may also allow for the remote support to be powered by the battery throughout the duration of the remote support, e.g. from 10 minutes up to several hours or more. Alternatively, the predetermined duration may allow for a remote computer to monitor the computer equipment, whilst the remote support device is powered from the battery and may thus be e.g. from 24 hours to 72 hours or more.

[0046] Often, computer equipment is connected to an uninterruptible power supply (UPS) to ensure a stable operation for a period of time when a power outage occurs. Connecting additional equipment, such as a portable remote support device, to the UPS may, however, compromise the operational stability of the computer equipment and is therefore not preferred. By the portable remote support device comprising the battery, computer equipment may be remote supported when power supply to the computer equipment is unstable and/or power outages occur.

[0047] In yet another embodiment, the remote support device may be adapted to connect to a virtual private network (VPN).

[0048] By providing a VPN-connection between the support device of the technician and the remote support device, the data is encrypted and thus more difficult for third parties to gain unauthorised access to. It will be clear to the person skilled in the art how a VPN-connection is established and used, as virtual private networks (VPNs) are very well known. VPN-connections and VPNs will therefore not be described in further detail.

[0049] In another embodiment, the network communication unit may be adapted to provide a network connection via satellite and/or via a mobile network.

[0050] According to this embodiment, the remote support device may be used to support computer equipment on locations where e.g. a local area network (LAN) through cable or Wi-Fi or 3G/4G is not available or cannot provide the necessary data bandwidth to transmit data from the remote support device to a remote computer of a technician with sufficiently low latency. Furthermore, computer equipment, such as routers and switches, that should provide a network connection in a computer environment, may be booted by or supported from boot by the remote support device. For instance, the portable remote support device may be equipped with a mobile data modem, such as a 3G, 4G or 5G data modem.

[0051] Alternatively or additionally, the network communication unit may be adapted to communicate with the cloud service via the Internet.

[0052] The portable remote support device may further comprise a serial port for connecting to equipment via a serial console. According to this embodiment, the portable remote support device may be connected to network equipment, such as routers, firewalls, relays, production machines, robots, etc. The technician will then be able to input text based commands to the network equipment via the serial port, e.g. in the form of applying or selecting appropriate settings, rebooting the equipment, running diagnostics, etc. Since only text based commands, and no data files, are communicated to the serial port in this manner, the risk of introducing malware or the like is minimised, or even eliminated.

[0053] According to a second aspect the invention provides a method for remote supporting computer equipment, the method comprising the steps of:

- providing a portable remote support device according to the first aspect of the invention,
- connecting the at least one output port of the remote support device to a pointing device input port and/or a keyboard input port of the computer equipment,
- connecting a video output port of the computer equipment to the video input port of the remote support device,
- connecting, by the network communication unit, the remote support device to a cloud service,
- obtaining a unique secure token,
- sharing the unique secure token among the remote support device and the cloud service,
- establishing a secure connection between a remote computer and the remote support device, via the cloud service, using the unique secure token,
- capturing by the video capturing unit of the remote support device a video output of the computer equipment and transmitting said captured video output to the remote computer via the established secure connection, and
- emulating on the at least one output port of the remote support device pointing device movements and/or keyboard key strokes, in response to input to the remote computer.

[0054] Thus, according to the second aspect, the invention provides a method for remote

supporting computer equipment. As described above with reference to the first aspect of the invention, the term 'computer equipment' should, in the present context, be interpreted broadly to cover, not only traditional computers, but also server, routers, robots, production equipment, etc.

[0055] In the method according to the second aspect of the invention, a portable remote support device according to the first aspect of the invention is initially provided. The remarks set forth above with reference to the first aspect of the invention are therefore equally applicable here.

[0056] Next, the at least one output port of the portable remote support device is connected to a pointing device input port and/or a keyboard input port of the computer equipment. Thereby pointing device signals and/or keyboard signals can be provided to the computer equipment by the portable remote support device, thereby allowing pointing device movements and/or keystrokes performed by a remotely positioned technician to be emulated and received at the computer equipment, as if the technician was present locally and operating the computer equipment directly in a normal manner.

[0057] Furthermore, a video output port of the computer equipment is connected to the video input port of the remote support device. Thereby a video feed can be provided to the remotely located technician, via the remote support device and the cloud service, as described above with reference to the first aspect of the invention.

[0058] Next, the remote support device is connected to a cloud service by the network communication unit of the remote support device. Accordingly, a connection is established between the remote support device and the cloud, allowing communication there between.

[0059] Next, a unique secure token is obtained, and the unique secure token is shared among the remote support device and the cloud service. For instance, the unique secure token may be generated by the remote support device and subsequently communicated from the remote support device to the cloud service, via the established connection. As an alternative, the unique secure token may be generated by the cloud service and subsequently communicated to the remote support device, via the established connection. As another alternative, the unique secure token may be generated by an external source which subsequently provides the unique secure token to the remote support device as well as to the cloud service, or to one of the remote support device and the cloud service. In the latter case, the entity which receives the unique secure token directly from the external entity subsequently communicates it to the other entity.

[0060] Thus, at this point in the process, the remote support device and the cloud service are both in the possession of the unique secure token.

[0061] Next, a secure connection is established between a remote computer and the remote support device, via the cloud service and using the unique secure token. In the present context

the term 'remote computer' should be interpreted to mean a computer which is arranged at a location which is remote relative to the location of the computer equipment which requires remote support. Establishing the secure connection could, e.g., include communicating the unique secure token to a remotely located technician via an alternative communication channel, e.g. by telephone, text message, via an app installed on a device, such as a cell phone, a tablet or a PC, or in any other suitable manner. The remotely located technician may then access the cloud service and enter the unique secure token, thereby gaining access to the remote support device, via the cloud service and the connection established between the remote support device and the cloud service. In order to provide an additional layer of security, access to the remote support device may further require that the technician enters a password or similar.

[0062] Once the secure connection between the remote computer and the remote support device has been established, it is possible for a technician located at the remote computer to access the portable remote support device, and thereby the computer equipment requiring remote support, via the remote computer and the secure connection.

[0063] Thus, a video output of the computer equipment is captured by the video capturing unit of the remote support device and transmitted to the remote computer via the established secure connection. Thereby the technician is able to view the video output of the computer equipment.

[0064] Furthermore, pointing device movements and/or keyboard key strokes are emulated on the at least one output port of the remote support device, in response to input to the remote computer. Accordingly, the technician can control the computer equipment requiring remote support by providing appropriate input to the remote computer and by means of the secure connection.

[0065] Consequently, a technician is able to see a video output of the computer equipment and control it by his/her remote computer through the remote support device. By emulating pointing device movements and keyboard key strokes on the at least one output port, no software or driver transfer to the computer equipment is necessary. Thus, the technician may support the device from boot and may e.g. enter and control a Basic Input/Output System (BIOS) and/or a Unified Extensible Firmware Interface (UEFI) of a piece of computer equipment. The pointing device movements may be emulated in response to e.g. a movement of a cursor, by e.g. a mouse, a touchscreen input, a visual tracking of a movement, or the like on a remote computer. The at least one output port may be configured as described in relation to the remote support device according to the invention.

[0066] The step of obtaining a unique secure token may be performed by the remote supporting device generating the unique secure token, and the step of sharing the unique secure token may comprise the remote supporting device communicating the generated unique secure token to the cloud service, via the network communication unit.

[0067] Alternatively, the step of obtaining a unique secure token may be performed by the cloud service generating the unique secure token, and the step of sharing the unique secure token may comprise the cloud service communicating the generated unique secure token to the remote supporting device, via the network communication unit.

[0068] In this case, the step of obtaining a unique secure token may further comprise the remote supporting device requesting a unique secure token. According to this embodiment, the unique secure token is generated in response to a request from the remote supporting device, e.g. in connection with initiating a remote support session.

[0069] The remote supporting device may further comprise a display, and the method may further comprise the step of displaying the unique secure token on the display. According to this embodiment, a trusted person located at the computer equipment requiring remote support is able to view the unique secure token at the display. Thereby the trusted person is able to communicate the unique secure token to a technician, e.g. via phone, text message or in any other suitable manner.

[0070] A unique secure token may be generated for each support session performed using the portable remote support device, e.g. each time the remote support device is powered on. As an alternative, a unique secure token may be generated at predefined time intervals, such as every 20 seconds, every 15 minutes, every hour, once a day, or any other suitable time interval. As another alternative, the unique secure token may be generated only once, e.g. during manufacture of the remote support device or the first time the remote support device is powered on. As another alternative, a unique secure token may be generated each time this is requested by a user or by the remote support device.

[0071] In an embodiment of the method, a battery of said portable remote support device in use acts as a power source of said remote support device, said battery being adapted to power the remote support device in use for a predetermined duration.

[0072] By a battery of the portable remote support device acting as a power source, the device may be used for supporting computer equipment in environments, where a power supply and/or the power net is unstable, as described with respect to the portable remote support device. Additionally, the portable remote support device may be moved between various pieces of computer equipment whilst remaining powered and connected to the remote computer of the technician.

[0073] In another embodiment of the method, the method comprises the step of:
moving the portable remote support device, powered by said battery, between different computers, wherein the remote support device remains connected to the remote computer via the computer network during the move.

[0074] By moving the portable remote support device between different computers, whilst the remote support device remains connected to the remote computer, less time is required to

support multiple pieces of electronic equipment, as no time is necessary to reconnect to the remote computer via the computer network. Additionally, the technician and the trusted person need not necessarily to remain in contact over e.g. a telephone, VoIP, instant messages, text messages, e-mail, or the like, as the technician may monitor, when the device is connected to the other computer, thus saving time.

[0075] In yet another embodiment of the method, the portable remote support device comprises a display, which displays a status of said remote support device, said status comprising network connection information and/or battery charge information, preferably state of charge (SoC) .

[0076] Consequently, the operating time on the battery supply may be estimated and charging may be planned and the device may be located such that latency and packet loss is minimised, as described in relation to the portable remote support system. By the network information being shown, it may be verified that the remote support device is online and/or connected to a remote computer of a technician, as described with respect to the portable remote support device.

[0077] In another embodiment of the method, the display of the portable remote support device further displays one or more of: a number of connected remote computers, pointing device connection information, video connection information, and/or keyboard connection information.

[0078] By providing connection information, the trusted person may be provided with some feedback in terms of, whether the equipment is connected correctly. Hence, the connection of the remote support device may be more intuitive and require less time and/or skill from the trusted person. Additionally, a guide on how to connect the remote support device may be displayed on the display, thus making the setup of the remote support device further intuitive.

[0079] The method according to the second aspect of the invention may, e.g., be performed in the following manner. When support to a certain piece of computer equipment is required, a unique secure token is obtained. The unique secure token may be generated at certain time intervals, in which case it is merely required that it is established what the currently valid unique secure token is. Alternatively, the unique secure token may be generated upon request and as a part of the initiation of the support session. The unique secure token may be generated by the portable remote support device, or it may be generated by an external source, e.g. a cloud service, and subsequently provided to the portable remote support device. The unique secure token may be displayed on a display of the portable remote support device. Alternatively, the unique secure token may be communicated to the trusted person in another manner, e.g. via an app installed on a cell phone, tablet, PC or the like connected to or associated with the portable remote support device.

[0080] The portable remote support device is connected to the computer equipment requiring support by connecting at least one output port of the remote support device to a pointing

device input port and/or a keyboard input port of the computer equipment, and by connecting a video output port of the computer equipment to a video input port of the remote support device.

[0081] The remote support device is connected to a cloud service, and the unique secure token is shared between the remote support device and the cloud service.

[0082] The trusted person then contacts a technician which is not located at the site of the computer equipment requiring support, and communicates the unique secure token to the technician, e.g. via telephone, text message, e-mail or in any other suitable manner.

[0083] The technician then accesses the cloud service, e.g. via a browser or via an app installed on a PC, a tablet, a cell phone or any other suitable device, enters the unique secure token, and thereby establishes a secure connection between a device operated by the technician and the portable remote support device. Accordingly, the technician gains access to the portable remote support device, via the cloud service and the secure connection. Since the portable remote support device is physically connected to the computer equipment requiring support, the technician also has access to the computer equipment. The portable remote support device may be password protected, in which case the technician will further have to enter a password in order to gain access to the portable remote support device.

[0084] The cloud service now acts as an intermediary server passing video streams from the portable remote support device to the device operated by the technician, thereby displaying the video on the device of the technician. Furthermore, input actions, such as mouse movements, mouse clicks, keyboard strokes, touch input, etc., performed by the technician are transmitted to the cloud service, which in turn sends such input to computer equipment, via the portable remote support device, thereby allowing the technician to control the computer equipment.

[0085] The different aspects of the present invention can be implemented in different ways including as a remote support device and a method for remote supporting a device as described above and in the following, each yielding one or more benefits and advantages described in connection with at least one of the aspects described above, and each having one or more preferred embodiments corresponding to the preferred embodiments corresponding to the preferred embodiments described in connection with at least one of the aspects described above.

[0086] Furthermore, it will be appreciated that embodiments described in connection with one of the aspects described herein may equally be applied to the other aspects.

BRIEF DESCRIPTION OF THE DRAWINGS

[0087] The invention will now be described in greater detail based on non-limiting exemplary

embodiments and with reference to the drawings, of which:

Fig. 1 shows a block diagram of an embodiment of a portable remote support device according to the invention,

Fig. 2 shows a perspective exterior view of an embodiment of a portable remote support device according to the invention, and

Fig. 3 shows a schematic drawing of a system comprising a portable remote support device according to the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0088] In Fig. 1, a block diagram of an embodiment of a portable remote support device 1 according to the invention is shown. The portable remote support device 1 comprises a control unit 10, a display unit 12, a user input device 14, a power management unit (PMU) 20, a battery 22, and a direct current (DC) power inlet 24. The portable support device 1 further comprises a first output port 32, a second output port 34, a video capturing unit 40, a video input port 42 and a network communication unit 50.

[0089] The PMU 20 is connected to the battery 22, the power inlet 24 and the control unit 10 and monitors parameters of the battery, such as voltage and temperature, to provide a state of charge (SoC) estimate of the battery 22 to the control unit 10. The battery 22 may comprise one or more lithium-ion (LIB) cells, lithium-ion polymer (LiPo) cells, lithium-air (Li-air) cells, nickel metal hybrid (NiMH) cells, or nickel cadmium (NiCd) cells, or any combination thereof. The PMU 20 initiates charging of the battery 22 when an external power source (not shown) is connected to the power inlet 24 and stops charging, when the battery 22 has reached a sufficient SoC, such as 95 %. The PMU 20 may further monitor the battery performance, e.g. maximum voltage and/or discharge curves, to estimate a state of health (SoH) or battery life time of the battery 22. In another embodiment, the PMU 20 may be integrated with the control unit 10 and/or the battery 22.

[0090] The control unit 10 is furthermore connected to the display unit 12 and the user input device 14. In another embodiment, the control unit 10 is connected to the display unit 12 through a video graphics card. The user input device 14 allows a user to e.g. power on and set up the remote support device 1 and may be a joystick, a multidirectional controller, a button, a keyboard, keypad, or any combination thereof.

[0091] Additionally, the control unit 10 is connected to a first 32 and second output ports 34, on which a pointing device signal and a keyboard signal is emulated. The first 32 and second output port 34 may be connected to a piece of computer equipment, such that e.g. the cursor and keyboard input of the computer equipment may be controlled by the remote support

device 1. The control unit 10 emulates the pointing device signal, e.g. a mouse signal, and the keyboard signal on the first 32 and second output ports 34, respectively, in response to an input from a remote computer (not shown) of a technician, to which the remote support unit 1 may be connected. In another embodiment, the signals on the first 32 and second output port 34 may be emulated based on an automated process stored in the remote support device 1 or transmitted to this by the remote computer. The first 32 and second output ports 34 may be unidirectional, allowing only communication from the remote support device 1 to the computer equipment or may be bidirectional, further allowing the computer equipment to communicate with the remote support device 1.

[0092] The video capturing unit 40 is connected to the video input port 42 as well as the control unit 10. The display output of a piece of computer equipment may be connected to the video input port 42. The video signal from the computer equipment is then processed by the video capturing unit 40 and transmitted to the connected remote computer of a technician through the control unit 10 and the network communication unit 50. As the display output video signal may be an analogue or a digital signal, the video capturing unit 40 may sample, downsample, upsample, and/or discretise the display output video signal from the computer equipment. The video capturing unit 40 and/or the control unit 10 may further compress and/or encrypt the video signal to reduce the necessary data bandwidth and/or security precautions of the communication connection to the remote computer of the technician. The video capturing unit 40 may be a video graphics card, a graphics processing unit (GPU), or a graphics capture card, or any combination thereof. In another embodiment, the video capturing unit 40 is integrated with the control unit 10.

[0093] The network communication unit 50 is connected to the control unit 10 and provides a network connection interface allowing the remote support device 1 to connect to a computer network. The network connection may be a wired connection, in which case a network connection port, e.g. an 8 position 8 contact (8P8C) connector for use with a Registered Jack 45 (RJ45) network communication or a 6 Position 2 Contact 6P2C for use with a Registered Jack 11 (RJ11) network communication, may be connected to the network communication unit 50. The network communication unit 50 may be an Ethernet network unit or a dial-up modem to provide a wired network connection. Alternatively, the network communication unit 50 may provide a wireless network connection, such as Wi-Fi (e.g. according to the IEEE 802.11-standard), 3G, 4G, LTE, and/or satellite network communication. The network connection may be an internet connection or may be a local network connection, such as a local area network (LAN) connection, or a VPN connection. The remote support device 1 and/or the network communication unit 50 may, hence, further include an antenna (not shown) adapted for use within a frequency band, e.g. 2.4 GHz and/or 5 GHz for Wi-Fi connections. The antenna may be integrated in an enclosure of the remote support device 1 or may be externally connected to the network communication unit through e.g. an antenna connection port, such as a coaxial port (not shown), connected to the network communication unit 50.

[0094] The control unit 10 controls the display 12, the user input device 14, the PMU 20, the video capturing unit 40, and the network communication unit 50 connected to it as well as

emulates the pointing device signal and the keyboard signal on the first 32 and second output port 34, respectively. The control unit may be a central processing unit (CPU), a microcontroller unit (MCU), a Digital Signal Processor (DSP), a field-programmable gate array (FPGA), or any combination thereof.

[0095] In Fig. 2, a perspective view of an embodiment of the portable remote support device 1' according to the invention is shown. The portable remote support device 1' is built up according to the block diagram in Fig. 1 and further comprises a network communication port 52 and a serial communication port 36. The first 16 and second buttons 18 are mechanical push buttons. In another embodiment, the buttons may be micro switches or capacitive touch buttons. The first button 16 acts as a power on/off button allowing the trusted person to turn the remote support device on and off. The second button 18 acts as an enter button allowing to confirm a choice from an on-screen menu. In other embodiments the functionality of the first 16 and the second button 18 may be reversed and/or the buttons 16, 18 may have other functions, e.g. allowing for reconnecting the device 1' to a network, or for rechecking if the cables have been correctly connected. The navigation button 14 may be used to navigate up, down, right, and/or left in an on-screen menu. In other embodiments, the remote support device may comprise fewer or more buttons, or the device may comprise a touchscreen instead of the display unit 12 and the buttons 14, 16, 18.

[0096] The display unit 12 comprises a liquid crystal display (LCD), connected to a control unit (not shown) of the remote support device 1' and shows, in use, status indicators showing network connection status, battery charge status, i.e. SoC, and port connection status for the individual input/output ports 24, 32, 34, 36, 42, 52 of the remote support device 1'. The display unit 12 may further be configured to show a unique secure token. The port connection status indicates, on which input/output ports 24, 32, 34, 36, 42, 52 a cable is inserted and communication is possible. Through the display unit 12, network connection settings, e.g. VPN-connection settings, DHCP-settings for IPv4- and IPv6-addresses for a LAN-connection, is shown and can be configured through the display unit 12 and the buttons 14, 16, 18. In another embodiment, the display unit 12 comprises a 3.5" light-emitting diode (LED) display and displays, in addition to the status indicators, the screen output of the computer equipment, when this is connected. The status indicators can be shown or hidden as overlays to the screen output of the computer equipment, or shown instead of the screen output. In another embodiment, the display unit 12 may comprise a thin-film-transistor (TFT) LCD, a light-emitting diode (LED) display, an organic LED (OLED) display, an active-matrix OLED display (AMOLED), or a quantum-dot LED (QLED) display, or any combination thereof. In another embodiment, the display unit 12 is a touchscreen and further includes a digitiser.

[0097] The power inlet 24 is a barrel-type connector for 5VDC power input from an external power source (not shown) to charge the battery. In another embodiment, the power inlet 24 may be a Universal Serial Bus (USB) compliant plug, such as a USB-A plug, a micro-USB plug, or a USB-C plug, a Thunderbolt-plug, a FireWire plug, or a 0.093"-standard connector, or any combination thereof. In another embodiment, a bus or rail voltage of the first 32 or second output port 34 or the serial communication port 36 may provide the power input to the PMU,

and the power inlet 24 may be omitted.

[0098] The first 32 and second output ports 34 of the remote support device 1' are a PS/2 mouse port and PS/2 keyboard port, respectively. Hence, only mouse and keyboard signals may be transmitted through the first 32 and second output port 34, respectively. Thereby the risk of malicious software being transmitted to the computer equipment is minimised. In another embodiment, the first 32 and second output ports 34 may be USB-ports, such as USB-A, USB-B, or USB-C, FireWire-ports, or serial communication ports, such as an RS-232, UART, or USART, or any combination thereof. USB-ports, however, are not preferred, as they may compromise security or security policies in vulnerable computer equipment environments, such as server environments. The serial port 36 is a 9-pin D-subminiature RS-232 port, which may be used to connect to network equipment such as routers, switches etc. The serial port 36 is connected to the control unit 10, which provides the communication with equipment connected through the serial port 36. In other embodiments, a plurality of serial ports may be connected to the control unit 10.

[0099] The video input port 42, which is connected to the video capturing device, is a 15-pin RS-232 port for connecting to a VGA-output of the computer equipment. In other embodiments, the video input port 42 may be a digital port, such as a Digital Visual Interface (DVI) port, a High-Definition Multimedia Interface (HDMI) port, or a DisplayPort, or any combination thereof.

[0100] Furthermore, the network communication port 52 is an 8P8C-connector for a RJ-45 compliant network connection. In another embodiment, this may be a 6P2C-connector for an RJ-11 compliant network connection. In other embodiments, the remote support unit 1' may comprise an antenna port for connecting to an external antenna, connected to the network communication unit, in combination with or instead of the network communication port 52. The antenna port may be a coaxial port, having e.g. a Sub-Miniature version A (SMA) connector, a Bayonet Neill-Concelman (BNC) connector, or a Type N connector.

[0101] In Fig. 3 a schematic drawing of a system 100 comprising a portable remote support device 1" according to the invention is shown. The remote support device 1" is connected to the computer equipment 110 by at least the first and second output port and video input port of the remote support device 1". The remote support device 1" is further connected to the remote computer 120 of the technician via a secure network connection 130. The remote computer 120 may be a server, a PC, a tablet-PC, a smartphone, and/or a Personal Digital Assistant (PDA). Furthermore, the network connection 130 may be a LAN-connection, a peerto-peer network connection, a VPN-connection, or a Personal Area Network (PAN) connection, or any combination thereof. The secure network connection 130 is established using a unique secure token, in the manner described above. Preferably, the technician may be identified and/or authorised to connect to the remote support device 1" by an IP-address of the remote computer 120 on the network provided by the network connection 130. The connection may be established through e.g. an application or a browser plug-in of the remote computer 120 or from a built-in feature in the operating system of the remote computer 120 or through a

browser. The pointing device and keyboard signal may be emulated by the remote support device 1" based on e.g. the mouse, touchpad, trackpad, stylus and/or finger input and keyboard, keypad or on-screen key input to the remote computer 120, respectively, from the technician. In some embodiments, the control unit of the remote support device 1", or an application or browser plug-in of the remote computer 120, may process the signal to adjust for e.g. differences in screen resolution and scaling between the computer equipment 110 and the remote computer 120. Furthermore, the technician may send commands, e.g. through a command prompt or terminal, which the remote support device 1" may forward to the computer equipment 110 through a serial port, or convert into pointing device movements or keystrokes and transmit to the computer equipment 110. Similarly, communication via e.g. a serial communication between a serial communication port of the remote support device 1" and the computer equipment 110 may be transmitted to the remote computer 120.

[0102] It should furthermore be emphasised that the term "comprises"/"comprising" when used in this specification is taken to specify the presence of stated features, integers, steps or components but not preclude the presence or addition of one or more features, integers, steps, components or groups thereof.

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US8595321B [0008]
- WO2013023195A [0012]
- US2007113267A [0013]

PATENTKRAV

1. Bærbar fjernsupport-indretning (1), som omfatter en processeringsenhed, en netværkskommunikationsenhed (50), som er indrettet til at kommunikere med en cloud-tjeneste, en videoopsamlingsenhed (40), i det mindste én videoinput-port (42) og i det mindste én output-port (32, 34), hvilken processeringsenhed er indrettet til at kommunikere videosignaler modtaget via videoinput-porten (42) til cloud-tjenesten via netværkskommunikationsenheden (50), og hvilken processeringsenhed er indrettet til at emulere pegeindretningssignaler og/eller tastatursignaler modtaget via netværkskommunikationsenheden (50) på den i det mindste ene output-port (32, 34), kendetegnet ved, at den bærbare fjernsupport-indretning (1) er indrettet til at modtage unikke sikre tokens fra cloud-tjenesten via kommunikationsenheden (50), og til at etablere en sikker forbindelse imellem fjernsupport-indretningen (1) og en fjern computer (120), via cloud-tjenesten og under anvendelse af det unikke sikre token.

2. Bærbar fjernsupport-indretning (1) ifølge et hvilket som helst af de foregående krav, hvor den bærbare fjernsupport-indretning (1) yderligere omfatter et display (12), som er indrettet til at vise en status for fjernsupport-indretningen (1).

3. Bærbar fjernsupport-indretning (1) ifølge krav 2, hvor displayet (12) yderligere er indrettet til at vise unikke sikre tokens.

4. Bærbar fjernsupport-indretning (1) ifølge et hvilket som helst af de foregående krav, som yderligere omfatter et batteri (22), som er indrette til at forsyne fjernsupport-indretningen (1) med strøm under brug for en forudbestemt varighed.

5. Bærbar fjernsupport-indretning (1) ifølge et hvilket som helst af de foregående krav, hvor den bærbare fjernsupport-indretning (1) er indrettet til at forbinde til et virtuelt privat netværk (VPN).

6. Bærbar fjernsupport-indretning (1) ifølge et hvilket som helst af de foregående krav, hvor netværkskommunikationsenheden (50) er indrettet til at tilvejebringe en netværksforbindelse via satellit og/eller via et mobilt netværk.

7. Bærbar fjernsupport-indretning (1) ifølge et hvilket som helst af de foregående krav, som yderligere omfatter en seriel port (36) til at skabe forbindelse til udstyr via en seriel konsol.

8. Fremgangsmåde til at yde fjernsupport til computerudstyr (110), idet fremgangsmåden omfatter trinnene til at:

- tilvejebringe en bærbar fjernsupport-indretning (1) ifølge et hvilket som helst af de foregående krav,
- forbinde den i det mindste ene output-port (32, 34) af fjernsupport-indretningen (1) til en input-port for en pegeindretning og/eller en input-port for et tastatur for computerudstyret (110), og
- forbinde en videooutput-port for computerudstyret (110) til videoinput-porten (42) af fjernsupport-indretningen (1),
kendetegnet ved, at fremgangsmåden yderligere omfatter trinnene til at:
- forbinde, ved hjælp af netværkskommunikationsenheden (50), den bærbare fjernsupport-indretning (1) til en cloud-tjeneste,
- cloud-tjenesten genererer et unikt sikkert token,
- dele det unikke sikre token mellem fjernsupport-indretningen (1) og cloud-tjenesten ved at cloud-tjenesten kommunikerer det genererede sikre token til fjernsupport-indretningen (1), via netværkskommunikationsenheden (50),
- etablere en sikker forbindelse imellem en fjern computer (120) og fjernsupport-indretningen (1), via cloud-tjenesten, under anvendelse af det unikke sikre token,
- opsamle, ved hjælp af videoopsamlings-enheden (40) af fjernsupport-indretningen (1), et video-output fra computerudstyret (110) og transmittere det opsamlede video-output til den fjerne computer (120) via den etablerede sikre forbindelse, og
- emulere, på den i det mindste ene output-port (32, 34) af fjernsupport-indretningen (1), pegeindretningsbevægelser og/eller tastaturanslag, som reaktion på input til den fjerne computer (120).

9. Fremgangsmåde ifølge krav 8, hvor trinnet til at opnå et unikt sikkert token yderligere omfatter, at fjernsupport-indretningen (1) anmoder om et unikt sikkert token.

10. Fremgangsmåde ifølge krav 8 eller 9, hvor fjernsupport-indretningen (1) yderligere omfatter et display (12), og hvor fremgangsmåden yderligere omfatter trinnet til at vise det unikke sikre token på displayet (12).

11. Fremgangsmåde ifølge et hvilket som helst af kravene 8-10, hvor et unikt sikkert token genereres for hver support-session, der udføres under anvendelse af den bærbare fjernsupport-indretning (1).

DRAWINGS

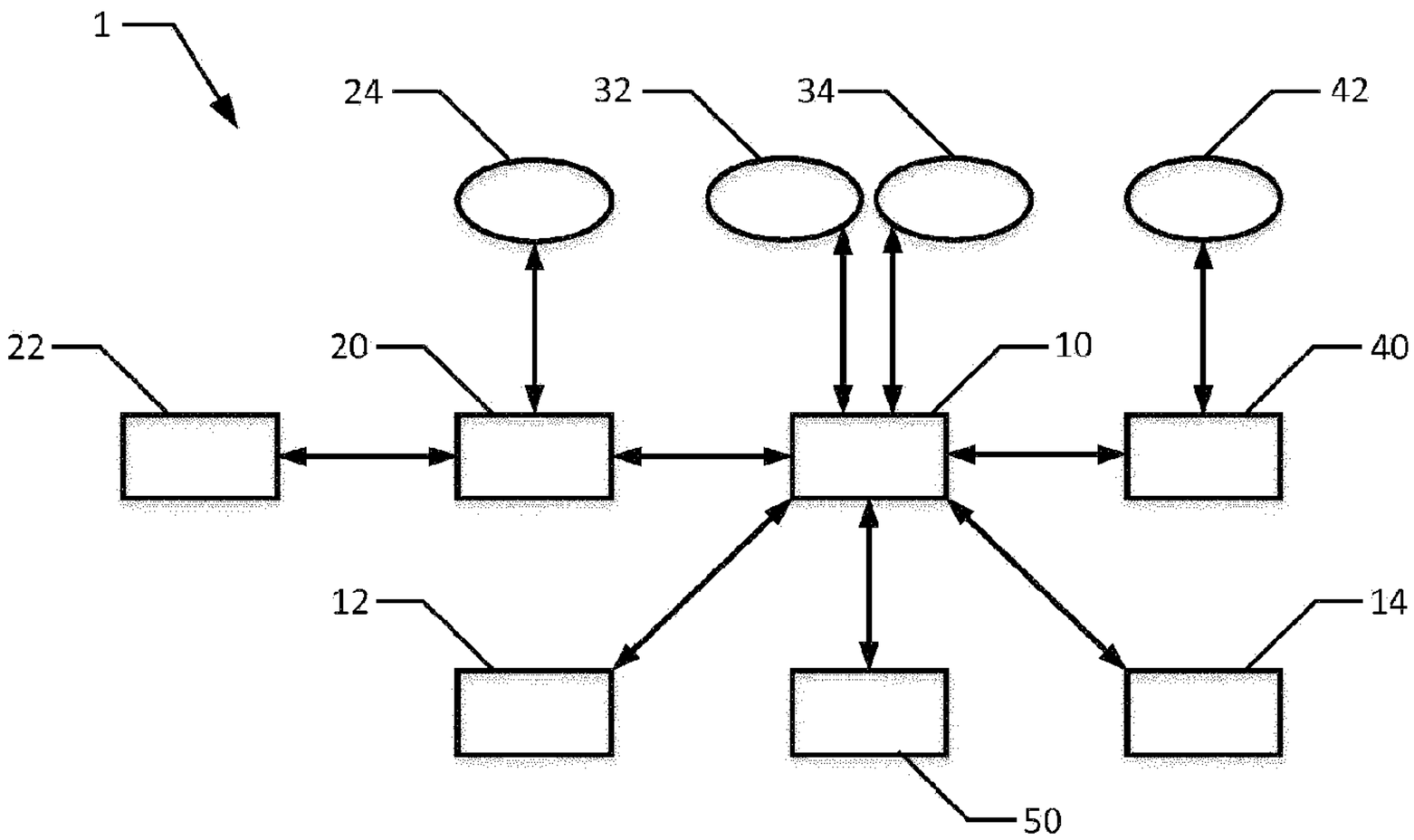


Fig. 1

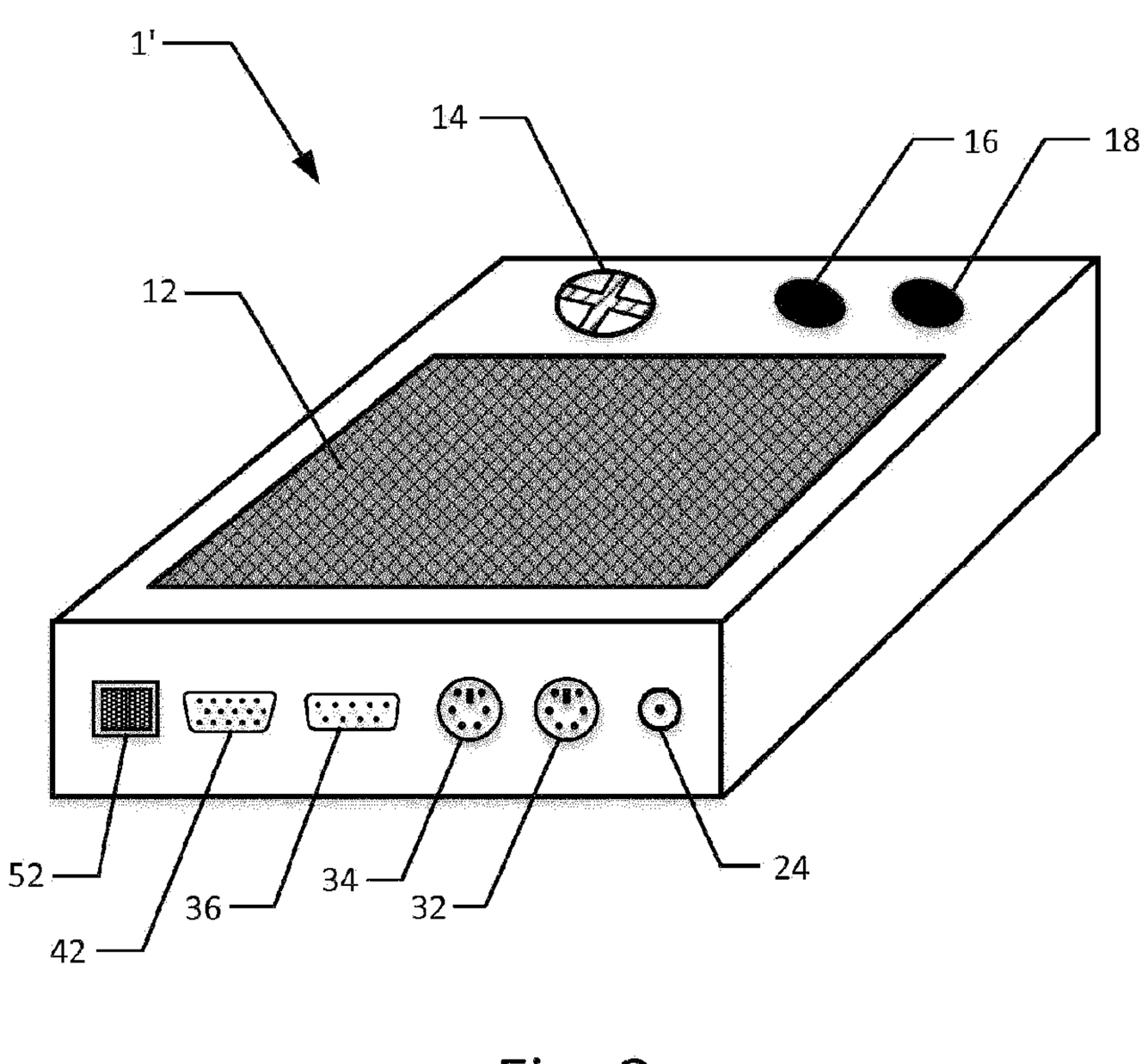


Fig. 2

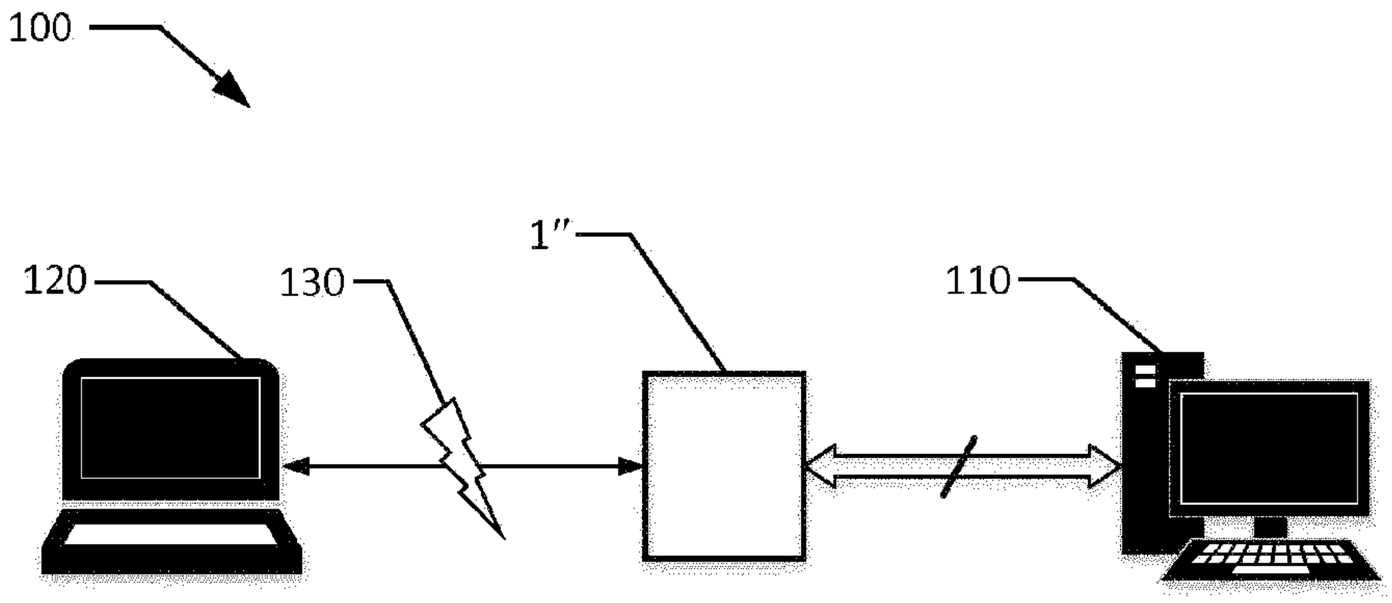


Fig. 3