(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 August 2017 (03.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/130068 A1

(51) International Patent Classification:
H04N 1/44 (2006.01) *B33Y 30/00* (2015.01)

(21) International Application Number:
PCT/IB2017/000130

(22) International Filing Date:
30 January 2017 (30.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/288,980 29 January 2016 (29.01.2016) US

(71) Applicant: **Y SOFT CORPORATION** [CZ/CZ]; U Knezske Louky 2151/18, 130 00 Prague (CZ).

(72) Inventors: **MUCHNA, Vaclav**; U Knezske Louky 2151/18, 130 00 Praha (CZ). **KRAJICEK, Ondrej**; Rakovecka 13a, 635 00 Brno (CZ). **MIKLAS, David**; Matejkova 2123/11, 190 00 Praha (CZ). **VLADIMIR, Coufal**; Merklovice 34, 517 54 Vamberk (CZ).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

WO 2017/130068 A1

(54) Title: SECURE 3D PRINTER AND 3D PRINTER MANAGEMENT NETWORK

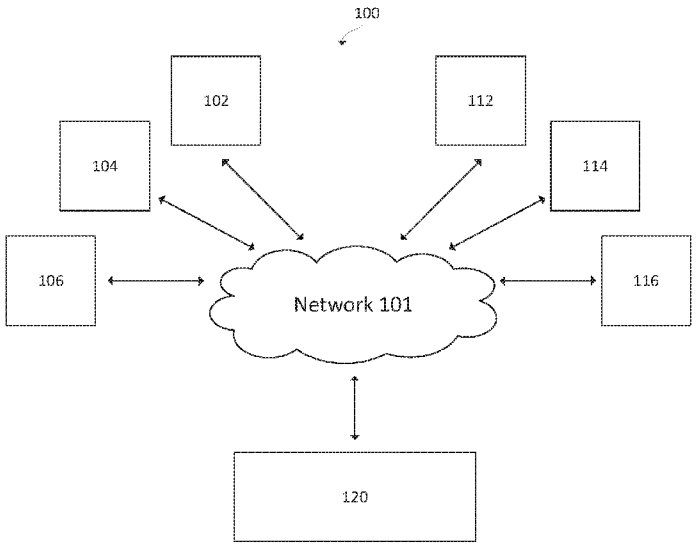


FIG. 1

(57) Abstract: A printer management system includes one or more printing devices having a printing area for printing according to a digital file, an access area through which a user may access the printing area, and a locking mechanism configured to lock the access area preventing access to the printing area. A management server is communicatively coupled to the one or more printing devices over a communication network and is configured to receive a print request from one or more user devices or one of the one or more printing devices to print the digital file, transmit the digital file to one of the one or more printing devices, and transmit commands to lock and unlock the locking mechanism of the one or more printing devices. In one embodiment the management system is configured to update a printing status of each of the one or more printing devices.

SECURE 3D PRINTER AND 3D PRINTER MANAGEMENT NETWORK

Cross Reference to Related Applications

[0001] This applications claims priority to U.S. Provisional Application No. 62/288,980, filed January 29, 2016, the contents of which are hereby incorporated by reference.

Field of the Invention

[0002] This invention generally relates to secure additive manufacturing, such as using 3D printers, and associated management networks.

Background of the Invention

[0003] 3D printing is an additive manufacturing process of making three dimensional solid objects from a digital file. One method for 3D printing is achieved by laying down successive layers of material until the three dimensional solid object is created. Each of these layers represents a thinly-sliced horizontal cross-section of the object. Other methods of 3D printing include selective laser sintering (SLS), selective laser melting (SLM), and stereolithography, among others. The 3D printing process begins by creating a virtual model of the object, typically a Computer Aided Design (CAD) file, and using specialized 3D printing software to "slice" the virtual model into hundreds or thousands of horizontal layers (depending on the desired fineness of the final printed object). The processed file with the sliced virtual model is then sent to a 3D printer that builds the model one layer at a time based on the individual slices of the virtual model.

[0004] Recent developments in 3D printing technology have reduced the cost and increased the availability of 3D printers and 3D printing software for the general public.

However, such 3D printers and software generally remain limited to a single locally connected device for individual personal or professional use. There is, therefore, an unmet demand for a 3D printer management network that is secure, centrally managed, and accessible to individuals all around the world.

Brief Description of the Invention

[0005] In one embodiment, a printer management system includes one or more printing devices that have a printing area for printing according to a digital file, an access area through which a user may access the printing area, a locking mechanism configured to lock the access area preventing the user from accessing the printing area, and a management server communicatively coupled to each of the one or more printing devices over a communications network. The management server is configured to receive a print request from one or more user devices or one of the one or more printing devices to print the digital file, transmit the digital file to a selected one of the one or more printing devices, and transmit commands to lock and unlock the locking mechanism of the one or more printing devices.

[0006] In one embodiment, the one or more printing devices are configured to lock the locking mechanism during printing of the digital file, and unlock the locking mechanism upon receiving a command from the management server or from an authorized user or upon an authorized user manually unlocking the locking mechanism. In another embodiment, the management server is further configured to update a printing status of each of the one or more printing devices and the selected one or more printing devices is selected based upon the printing status of each of the one or more printing devices.

[0007] In one embodiment, the one or more printing devices further comprises a user interface. The user interface is configured to authenticate an authorized user, and unlock the locking mechanism in response to an unlock command from the authorized user.

[0008] In one embodiment, the locking mechanism comprises an electromagnetic lock. In another embodiment, the locking mechanism comprises a mechanical bolt-action lock.

[0009] In one embodiment, the management server is further configured to store a plurality of digital files, and the user interface is further configured to retrieve, in response to a request from the authorized user, a selected one or more digital files of the plurality of digital files for printing by the printing device.

[0010] In one embodiment, the user interface is further configured to transmit, in response to a print command from the authorized user, the print request to the management server. In another embodiment, the print request comprises the metadata for the digital file.

[0011] In one embodiment, the metadata comprises at least one of a file name of the digital file, an owner of the digital file, an estimated time to print the digital file, and an estimated amount of material required to print the digital file. In another embodiment, the printing status indicates printer operation time, printer occupation time, or printer material remaining.

[0012] In one embodiment, the one or more printing devices further comprises a moveable panel adapted to cover the access area when disposed in a closed position, and the locking mechanism is configured to lock the moveable panel in the closed position.

[0013] In one embodiment, a printer management system includes, a management server capable of being communicatively coupled to one or more printing devices over a communications network, The management server is configured to receive, over the communications network, a print request from one or more user devices or the one or more printing devices to print a digital file, transmit, over the communications network, the digital file to a selected one or more printing devices, and transmit, over the communications network, commands to lock and unlock a locking mechanism of the one or more printing devices. The locking mechanism is configured to secure an access area through which a user may access a printing area of the printing device for printing the digital file.

[0014] In one embodiment, the management server transmits the command to lock the locking mechanism of the selected one or more printing devices prior to printing of the digital file, and transmits the command to unlock the locking mechanism of the selected one or more printing devices at a time after the digital file has completed printing.

[0015] In one embodiment, the management server is further configured to update a printing status of each of the one or more printing devices. In another embodiment, the management server is further configured to store the digital files received from the one or more user devices. In one embodiment, the print request comprises the metadata for the digital file.

[0016] In one embodiment, metadata comprises at least one of a file name of the digital file, an owner of the digital file, an estimated time to print the digital file, and an estimated amount of material required to print the digital file. In another embodiment,

the printing status indicates printer operation time, printer occupation time, or printer material remaining.

[0017] In one embodiment, a printing device includes a printing area for printing a digital file, an access area through which a user may access the printing area, and a locking mechanism configured to lock the access area preventing the user from accessing the printing area. The printing device is capable of being communicatively coupled to a management server, and the printing device is configured to lock the locking mechanism during printing of the digital file, and unlock the locking mechanism upon receiving a command from an authorized user or from the management server.

[0018] In one embodiment, the locking mechanism comprises an electromagnetic lock. In another embodiment, the locking mechanism comprises a mechanical bolt-action lock. In one embodiment, the printing device includes a user interface configured to authenticate an authorized user, and unlock the locking mechanism in response to an unlock command form the authorized user.

[0019] In one embodiment, the printing device also includes a moveable panel adapted to cover the access area when disposed in a closed position, wherein the locking mechanism is configured to lock the moveable panel in the closed position.

Brief Description of the Figures

[0020] FIG. 1 is a block diagram of a 3D printer management network, according to one embodiment of the invention.

[0021] FIG. 2 is a block diagram of the structure of a management server of the 3D printer management network of FIG. 1, according to one embodiment of the invention.

[0022] FIG. 3 is a block diagram of the structure of a 3D printer of the 3D printer management network of FIG. 1, according to one embodiment of the invention.

[0023] FIGS. 4A-4G are diagrams of a 3D printer, according to one embodiment of the invention.

[0024] FIGS. 5A-5I are screen images of the user interface of an additive printer, such as a 3D printer, according to one embodiment of the invention.

[0025] FIG. 6 is a flowchart of method steps for securely printing a 3D printing file using the 3D printer management network of FIG. 1, according to one embodiment of the invention.

[0026] FIGS. 7A-7E are screen images of the user interface of a user device of the additive printer management network of FIG. 1, according to one embodiment of the invention.

[0027] FIGS. 8A-8K are screen images of the administrator interface of a management server of the additive printer management network of FIG. 1, according to one embodiment of the invention.

Detailed Description of the Invention

[0028] FIG. 1 is a block diagram of a 3D printer management network 100, according to one embodiment of the invention. As shown in FIG. 1, network 101 connects a plurality of user devices 102, 104, and 106, a management server 120, and a plurality of 3D printers 112, 114, and 116. In one embodiment, the management server 120 may be run on one or more of the 3D printers 112, 114, or 116 within the 3D printer management network 100. For illustrative purposes, FIG. 1 illustrates three 3D printers 112, 114, and 116 but many more could be implemented in the network 100. The network 101 may be any known communications network, including the Internet, a Local Area Network (LAN), a Wide Area Network (WAN), etc. User devices 102, 104, and 106 may

comprise any suitable device for transmitting a request for 3D printing over the network 100. For example, user devices 102, 104, and 106 may comprise personal computers (PCs), laptops, smartphones, tablets, and the like. Management server 120 may also comprise any suitable device for managing the plurality of 3D printers 112, 114, and 116 over the network 101, including a PC, a laptop, a rackmount system mounted in a server cage, etc.

[0029] Because network 101 connects the plurality of user devices 102, 104, and 106, the management server 120, and the plurality of 3D printers 112, 114, and 116, the devices comprising the secure 3D printer network 100 may be distributed geographically as necessary. For example, in one embodiment, 3D printers 112, 114, and 116 may be located remotely from the management server 120, which in turn, is located remotely from the user devices 102, 104, and 106. Given the distributed nature of the 3D printer management network 100, in one embodiment, the communications between the plurality of user devices 102, 104, and 106, the plurality of 3D printers 112, 114, and 116, and the management server 120 over the network 101 are secured using any suitable technique. In various embodiments, the communications may be secured using public key cryptography such as RSA, Transport Layer Security (TLS), Secure Sockets Layer (SSL), or any combination or variant thereof.

[0030] While FIG. 1 shows three user devices 102, 104, and 106, and three 3D printers 112, 114, and 116, it should be understood that the 3D printer management network 100 is not limited to any specific number of user devices and 3D printers, and is scalable from a single user device and a single 3D printer, to hundreds or thousands, or more, of such devices. Additionally, central server 120 may comprise a single device, or

in other embodiments, may comprise multiple devices centrally managing the plurality of 3D printers 112, 114, and 116.

[0031] FIG. 2 shows a block diagram of the structure of the management server 120 of the 3D printer management network 100 shown in FIG. 1, according to one embodiment of the invention. As shown in FIG. 2, the management server 120 comprises a processor 202 in communication with DRAM 204, persistent storage 206, peripheral interface 208, and network interface 210. In another embodiment, the persistent storage 206 need not be persistent, and may comprise volatile memory devices, or a combination of volatile and non-volatile memory devices. In yet a further embodiment, the persistent storage 206 and the DRAM 204 may be the same device.

[0032] Network interface 210 connects the management server 120 to the network 101. Peripheral interface 208 connects the management server 120 to peripheral input devices 201. Peripheral interface devices 201 may include a keyboard, a mouse, a touch panel, or any other suitable device to input user commands and control the management server 120. Alternatively, in one embodiment, control of the management server 120 is performed remotely over the network 101 through the network interface 210. Persistent storage 206 stores user account subsystem 212, security subsystem 214, and 3D printer management subsystem 216.

[0033] User account subsystem 212 stores individual user account information, including the user's 3D printing history, stored 3D printing files, available funds, and any pending 3D printing requests. In one embodiment, the individual user account information is stored remotely and the user account subsystem 212 is configured to access the remotely stored information by causing the processor 202 to retrieve the

information through the network 101 via the network interface 210. In this embodiment, the individual user information may be stored in the cloud, in a network-attached storage (NAS) device, or any other suitable remote storage device. For enhanced security, in one embodiment, the individual user information is encrypted using any suitable method.

[0034] Security subsystem 214 stores user authentication information with respect to each individual's user information stored by the user account subsystem 212. The user authentication information may comprises a user's username and associated password, a user's identification and associated pin number, a user's card number, a user's RFID tag, a user's biometric data (such as a fingerprint image), or any other suitable identification information, or combination thereof, to verify the user is properly authorized to access the user information stored or accessible by the user account subsystem 212. In one embodiment, the user authentication information is stored remotely from the management server 120, and the security subsystem 214 is configured to access the remotely stored authentication information by causing the processor 202 to retrieve the information through the network 101 via the network interface 210. In this embodiment, the user authentication information may be stored in any suitable remote storage device. In one embodiment, the user authentication information is encrypted using any suitable method.

[0035] Additionally, security subsystem 214 stores administrator authentication information. Once authenticated, the security subsystem 214 is configured to allow the administrator to access all of the individual user account information stored or accessible by the user account subsystem 212. Once given access to the individual user account information, an administrator may view or modify the user account information. Additionally, in one embodiment, the security subsystem 214 is configured to allow the

administrator to lock or unlock a user's account. For example, if a user has violated a rule or regulation imposed by an administrator, the administrator may lock the user's account to prevent the user from accessing the secure 3D printer network 100.

[0036] 3D printer management subsystem 216 is configured to retrieve and make available real-time information regarding the status of the 3D printers 112, 114, and 116 of the secure 3D printer network 100 (shown in FIG. 1) to both the authorized users and the administrators. In one embodiment, the 3D printer management subsystem 216 is configured to either periodically or asynchronously fetch the status of each individual 3D printer 112, 114, and 116 to determine if a respective 3D printer 112, 114, and 116 is idle (available to receive and print a 3D printing file), is in progress (in the process of printing the 3D printing file), is completed (printing has been completed but the user has not retrieved the printed object), has encountered an error, or requires maintenance, among other statuses that may also be applicable to each of the 3D printers 112, 114, and 116.

[0037] Additional status information, such as the amount of printer material remaining (e.g., length of filament string) , the estimated time remaining for the 3D printing to be completed, printer operation time (indicating total for the 3D printing to complete), total occupation time including print time and the amount of time the 3D printing has been finished (indicating the amount of time the object has been waiting to be picked up by the user), and the estimated amount of time before a user picks up the 3D printed object (can be an estimate based on the average pickup time, or an estimated pick up time provided by the user, for example) may also be provided to users and administrators.

[0038] In another embodiment, the plurality of 3D printers 112, 114, and 116 periodically transmit their current status over the network 101 to the management server

120, and the 3D printer management subsystem 216 is configured to cause the processor 202 to retrieve that information via the network interface 210 for use by the 3D printer management subsystem 216. In one embodiment, the real-time information regarding the status of the 3D printers 112, 114, and 116 of the secure 3D printer network 100 is stored in the DRAM 204.

[0039] In one embodiment, the management server 120 is configured to receive a 3D printing request to print a 3D printing file from a user device 102, 104, or 106, and associates the 3D printing request and 3D printing file with the user's account. After the 3D printing request and 3D printing file is received by the management server 120, the user may then access the 3D printing file from one of the 3D printers 112, 114, and 116 for printing by logging into their account and retrieving the 3D printing file from the management server 120.

[0040] In another embodiment, 3D printing files containing metadata for the 3D print job (i.e., the details of the print job, including the print job file name, the estimated amount of time to print, material consumption, owner of the print job, and a unique identifier that allows the management server 120 to associate user account information with a specific 3D print job) may be stored on and retrieved from any portable storage device connected to one of the 3D printers 112, 114, and 116. In this embodiment, the 3D printers 112, 114 and 16 are configured to retrieve and store the metadata for the 3D print job in a non-volatile memory (not shown) along with user account information and any status updates related to the print job. The 3D printers 112, 114 and 116 send the metadata for the 3D print job to the management server 120 when communication can be established with the management server 120 over network 101. Alternatively, the

metadata may be separately transmitted to the management server 120 from a user device 102, 104, or 106 when communication can be established with the management server 120 over network 101.

[0041] In yet a further embodiment, 3D printing files may be generated by additional devices, such as 3D scanners or X-ray imagers, and the files may be transmitted to the management server 120, transmitted to a user device 102, 104, or 106, or retrieved using a portable storage device for 3D printing. Depending on the method of transmission and/or retrieval of the 3D printing files generated in this manner, either of the embodiments described above may be utilized to initiate a 3D printing request for the 3D printing file.

[0042] In another embodiment, the management server 120 is configured to receive a 3D printing request from a user device 102, 104, or 106 of an authorized user over the network 101, and directly transmit the 3D printing file specified by the user to a selected 3D printer 112, 114, and 116 of the secure 3D printer network 100. In one embodiment, the user may view the status of the 3D printers 112, 114, and 116, and select one or more of the 3D printers 112, 114, and 116 to print the 3D printing file. In another embodiment, the user may specify how many copies of the 3D printing file the user wants to print, and the management server 120 dynamically selects the 3D printers 112, 114, and 116 to transmit the 3D printing file to for printing. In this embodiment, the management server 120 may dynamically select the 3D printers 112, 114, and 116 based upon the real-time information regarding the status of each of the 3D printers 112, 114, and 116.

[0043] In one embodiment, the management server 120 is configured to allow an administrator to remotely take control of any 3D printer 112, 114, and 116 of the secure

3D printer network 100. An administrator may cancel any pending print job, whether in progress or awaiting printing, re-arrange pending print jobs, power up, shut down, or restart the 3D printers 112, 114, and 116, and lock or unlock 3D printers 112, 114, and 116 (discussed in further detail below in connection with FIG. 3).

[0044] FIG. 3 is a block diagram of the structure of a 3D printer 112 of the 3D printer management network 100 of FIG. 1, according to one embodiment of the invention. As shown in FIG. 3, the 3D printer 112 comprises a processor 302 in communication with a secure memory 304, user interface 308, 3D printing area 306, and network interface 310. Network interface 310 connects the 3D printer 112 to the network 101. 3D printing files that are received over the network 101 via the network interface 310 are stored in the secure memory 304. Secure memory 304 may either be persistent or non-persistent memory, or both. Because the 3D printer 112 must be publicly accessible, secure memory 304 may be electronically or physically secured, or both, to protect the integrity and security of the user's 3D printing files. Electronic security for the secure memory 304 may comprise any suitable encryption techniques. Physical security for the secure memory 304 may comprise locking the secure memory 304 in a secure location within the 3D printer 112.

[0045] 3D printing area 306 comprises the 3D printing structure of the 3D printer 112. 3D printing area 306 includes, for example, a print head (also known as an extruder) mounted to a plurality of motors that control the spatial movement of the print head in the x, y, and z axis, and a controller configured to control the motors and the print head to print the layers of a 3D printing file. 3D printing area 306 may comprise structures suitable for any known 3D printing process, including vat photopolymerisation, material

jetting, binder jetting, material extrusion, powder bed fusion, sheet lamination, directed energy deposition, etc.

[0046] The 3D printing area 306 is secured using a locking mechanism to prevent unauthorized access to the 3D printing area 306. The locking mechanism may comprise any suitable locking device for securing the 3D printing area 306. In one embodiment, the locking mechanism comprises an electromagnetic lock. In another embodiment, the locking mechanism comprises a mechanical bolt action lock. The 3D printing area 306 may only be unlocked by the owner of the 3D printing file using his or her user authentication information, or by an administrator. The locking mechanism may also generate visual, audible and/or tactile alerts when an unauthorized user attempts to unlock or damage the lock.

[0047] User interface 308 provides an interface for a user or an administrator to control aspects of the individual 3D printer 112, or in various embodiments, aspects of the secure 3D printer network 100 may be accessed via the user interface 308. In one embodiment, the user interface 308 allows a user to enter his or her user authentication information to unlock the 3D printing area 306. Depending on the type of user authentication information required, the user interface 308 may include a card reader, an RFID scanner, a biometric scanner, etc. Additionally, in another embodiment, once the user provides valid authentication information to the user interface 308, the user may access the user account subsystem 212 of the management server 120 (shown in FIG. 2) over the network 101 to access his or her user information.

[0048] From the user interface 308, an authorized user may retrieve a 3D printing file associated with the user's account from the management server 120 for printing, view the

user's print requests and print history, send stored 3D printing files to other users or groups of users, access 3D printing files shared with the user from another user, request a previously printed file to be sent to the 3D printer 112, or any other 3D printer 114 and 116 within the secure 3D printer network 100, for printing, view the user's account balance, add funds to the user's account, upload a new 3D printing file from a local storage device (such as a USB drive) for printing, etc. In one embodiment, an authorized user may also download a 3D printing file from a database of 3D printing files. In this embodiment, the database may be available for specific users. 3D printing files in the database may be filtered depending on, for example, the age of the users or the types of groups to which they belong. In one embodiment, users that contribute to the 3D printing files in the database may be compensated or rewarded, either in money, printing credit, or in any alternative method of remuneration, for their contribution to the database. In effect, the user interface 308 may be configured to provide the authorized user the same functionality as the user's devices 102, 104, or 106.

[0049] Similarly, in one embodiment, an administrator may use the user interface 308 to access user account subsystem 212, the security subsystem 214, and the 3D printer management subsystem 216 of the management server 120 via the network 101. In this manner, the administrator may effectively manage the secure 3D printer network 100 from 3D printer 112. For example, if an administrator notices that an error occurred during the printing of a 3D printing file, the administrator may use the user interface 308 to access the account subsystem 212 of the management server 120 and issue a refund to the account of the user that requested the printing.

[0050] In another embodiment, the user interface 308 may further include an option to request assistance from an administrator or an authorized staff member. In one embodiment, the user may request electronic assistance, whereby a communications link is opened to an administrator or an authorized staff member in order to provide assistance. In one embodiment, the user may request physical assistance, whereby an electronic or physical message (for example, a flashing light on the 3D printer 112) is transmitted to an administrator or an authorized staff member indicating that physical assistance is requested at the 3D printer 112. In one embodiment, the administrator and authorized staff members that are authorized to provide assistance can be configured on the management server 120.

[0051] FIGS. 4A-4G are diagrams of a 3D printer of the 3D printer management network 100 of FIG. 1, according to one embodiment of the invention. FIG. 4A shows a side elevational view of the 3D printer. In FIG. 4A, the top panel of the 3D printer has been removed, and both the filament access panel 402 as well as the door to the 3D printing area 404 are opened. Both the filament access panel 402 as well as the door to the 3D printing area 404 may be locked to prevent unauthorized access. In one embodiment, only an administrator may open the filament access panel 402. An authorized user may open the door to the 3D printing area 404 by using their authentication information (discussed in greater detail below). Both the filament access panel 402 and the door to the 3D printing area 404 may be unlocked by an administrator locally or remotely via the management server of the 3D printer management network.

[0052] FIG. 4B shows a top elevational view of the 3D printer. As shown in FIG. 4B, a 3D printing head 406 is positioned above a 3D printing tray 408. FIG. 4C shows a side

profile view of the 3D printer. In FIG. 4C, the door to the 3D printing area 404 is closed. A window 410 in the door allows users and administrators to visually monitor and inspect the 3D printing process without opening the door to the 3D printing area 404. In other embodiments, the window 410 may be configured to be transparent or opaque. In this embodiment, for example, the window 410 may be opaque during the printing of the 3D model to maintain confidentiality and security, and will turn transparent only after the user or an administrator logs into the 3D printer.

[0053] FIG. 4D shows another side profile view of the 3D printer. In FIG. 4D, the door to the 3D printing area 404 is opened. FIG. 4D provides another view of the position of the 3D printing head 406 and the 3D printing tray 408 shown in FIG. 4B. The locking mechanism 412 for the door of the 3D printing area is encircled in FIG. 4D. As shown in FIG. 4D, the locking mechanism 412 is an electromagnetic lock. As previously discussed, in other embodiments, the locking mechanism for the door of the 3D printing area can be any suitable locking mechanism.

[0054] FIG. 4E shows another side elevational view of the 3D printer. In FIG. 4E, the top panel of the 3D printer is present, and both the filament access panel 402 and the door to the 3D printing area 404 are closed. As shown in FIG. 4E, a card reader 414 is located on the top right corner of the 3D printer. FIG. 4F shows a top view of the top right corner of the 3D printer. In FIG. 4F, the top panel of the 3D printer is removed, and the card reader 414 can be seen. FIG. 4G is another side elevational view of the 3D printer. In FIG. 4G, the user interface of the 3D printer 416 has been extended from underneath the 3D printer for use by a user or administrator.

[0055] FIGS. 5A-5I are screen images of the user interface of a 3D printer, according to one embodiment of the invention. FIG. 5A shows a default authentication screen instructing the user to swipe the user's card in order to login. FIG. 5B shows the PIN authentication screen after a user has swiped his or her card. Once the user enters the correct PIN, FIG. 5C shows the user's account screen. As shown in FIG. 5C, the user "John Doe" has previously sent a request to 3D print a 3D printing file entitled "Spiral Vase" to a management server 10 minutes ago. As previously discussed, once an authorized user is logged in, the user interface of the 3D printer will retrieve the user's account information from the management server, including any requested print jobs (and associated metadata such as estimated time to print and cost to print), the user's account balance, etc. In Fig. 5C, John Doe's account screen also displays an estimated time to print the Spiral Vase is 2 hours and 22 minutes, and will cost John Doe $2.50 to print. John Doe's account balance can be seen at the top right corner of the user's account screen.

[0056] In FIG. 5D, user John Doe selects the Spiral Vase for printing. FIG. 5E shows an instruction screen instructing John Doe to open the door to the 3D printing area of the 3D printer to prepare the 3D printer for printing. In one embodiment, glue needs to be applied to 3D printing tray and the 3D printer needs to be calibrated prior to printing. FIG. 5F shows a printing status screen indicating the current information of the printing of the Spiral Vase. Status information includes the print time, time remaining, percentage completion, and temperature readouts of various components of the 3D printer. The printing status screen also includes options to stop printing and to call the admin if the user detects an issue during printing.

[0057] In FIG. 5G, a printing finished screen notifies user John Doe that Spiral Vase has completed printing. After the printing is complete, John Doe may demand a refund if he is unsatisfied with the printed Spiral Vase, or if he is satisfied, he can unlock the door to the 3D printing area and retrieve his printed Spiral Vase. The printing finished screen includes a camera image from the back of the 3D printing area, which in combination with the windowed door, provides users up to a 360 degree view of the printed object to determine if they are satisfied with the printed object. In another embodiment, the camera may be positioned in front of the printing area or in any other portion of the printing area.

[0058] FIG. 5H shows a call admin screen. As previously shown in FIG. 5F, during printing the user may call the admin for assistance. As shown in FIG. 5H, there are a number of different issues that may occur during the 3D printing process. A number of these issues are identified for the user in the form of shortcut buttons, and if the user is not experiencing any of the preset issues, the user may select the "other" button and may be given the option to describe the issue. FIG. 5I shows an admin notification screen. In FIG. 5I, after the user selects the issue on the call admin screen (shown in FIG. 5H), the user is informed that an administrator has been notified of the issue, and is given an estimated time for an administrator to come and address the issue identified by the user.

[0059] FIG. 6 is a flowchart of method steps 600 for securely printing a 3D printing file using the 3D printer management network 100 of FIG. 1, according to one embodiment of the invention. At step 602, a request for 3D printing of a 3D printing file is transmitted from a user to the management server. In one embodiment, the request

may be sent from a user device. In another embodiment, the request may be sent from the user interface of a 3D printer within the 3D printer management network.

[0060] At step 604, a user logs into his or her user account from a 3D printer and selects the previously transmitted printing file to be printed. The 3D printer retrieves the 3D printing file from the management server 120. At step 606, the management server checks the user account information of the user and determines if the user has sufficient funds for printing the user's 3D printing file. The estimated cost of printing a 3D printing file may be based on an estimated amount of time it takes the print the 3D printing file, an estimated amount of material required to print the 3D printing file, the complexity of the 3D printing file, or any combination of any relevant cost considerations. At step 608, if the management server determines there are insufficient funds in the user's account, the management server will send a request to the user to add funds to the user's account.

[0061] At step 610, if the management server determines the user has sufficient funds to print the 3D printing file, the user's account will be deducted the estimated amount for printing the 3D printing file. The user then prepares the 3D printing area of the 3D printer for printing. In one embodiment, the user must apply an adhesive to a 3D printing tray below a 3D printing head of the 3D printer, and calibrate the 3D printer prior to printing. In another embodiment, adhesive may not be required. After the 3D printer has been prepared, the 3D printing area of the selected 3D printer is locked, and the 3D printer begins printing the 3D printing file. The 3D printer updates its status from idle to in progress, and in one embodiment, transmits its status to the management server. In another embodiment, the management server incrementally deducts the total cost of the print job from the user's account as the printing process progresses.

[0062] At step 612, the 3D printing is completed, the 3D printer updates its status to printing completed, and the user is notified. In one embodiment, the user may be notified directly by the 3D printer. In another embodiment, the 3D printer transmits a message to the management server, which then sends a success notification to the user. The user notification may be sent to the using any suitable method, including via a text message, email, an automated phone message, or any other suitable method, or any combination thereof.

[0063] At step 614, the user inspects the printed object and determines if he or she is satisfied with the print job. In one embodiment, this determination may be made by visually observing the 3D printed object. At step 616, if the user is not satisfied with the print job, the user may demand a refund. At step 618, if the user is satisfied with the print job, the user provides his or her authentication information to the 3D printer. As previously discussed in connection with FIG. 2, the user's authentication information may comprise a user's username and associated password, a user's identification and associated pin number, a user's card number, a user's RFID tag, a user's biometric data, or any other suitable identification information, or combination thereof. In one embodiment, the user may enter their authentication information via the user interface of the 3D printer.

[0064] At step 620, if the user provides valid authentication information, the 3D printing area of the 3D printer is unlocked and the user may retrieve the 3D printed object. If the user is unable to provide valid authentication information, the user is prompted to try again. If the user is unable to provide valid authentication information after a number of attempts, in one embodiment, the user's account is locked and the user

must seek an administrator to unlock the user's account. After the user retrieves the 3D printed object, the actual cost of the print job (based on the amount of time and material used) will be calculated and the actual cost will be billed to the users account. For example, if at step 606 the estimated amount is greater than the actual cost of printing, then the user's account will be credited the difference. Conversely, if the estimated amount is less than the actual cost of printing, then the user's account will be deducted the difference.

[0065] FIGS. 7A-7E are screen images of the user interface of a user device of the 3D printer management network 100 of FIG. 1, according to one embodiment of the invention. FIG. 7A shows a 3D file selection screen of the user device. A user may select a 3D file to print by selecting the file name, and selecting the "Open object" button. FIG. 7B shows a preview screen with a 3D model of the selected 3D file for printing. The user may modify the 3D model from the preview screen shown in FIG. 7B prior to printing. If the user is satisfied with the 3D model for printing, the user may select the continue button. FIG. 7C shows a print parameter screen. The user may select the material, print quality, speed, and slicer used to print the 3D model. Additionally, depending on the shape of the 3D model, the user may optionally elect to print supports along with the 3D model.

[0066] FIG. 7D shows a processing screen indicating that the user device is processing the 3D model for printing using the parameter selected by the user. In one embodiment, preparing the 3D model includes slicing the model, generating supports (if elected), generating and optimizing the printing instructions for the 3D printer. FIG. 7E shows a print request screen. After the 3D model has been processed into a 3D printing file, the

user may send the print request along with the 3D printing file to the management server. After the print request is sent to the management server, the user can then use any 3D printer from the 3D printer management network 100 to retrieve the 3D printing file from the management server and print the 3D model as previously discussed in connection with FIGS. 5A-5I.

[0067] FIGS. 8A-8K are screen images of the administrator interface of a management server of the 3D printer management network 100 of FIG. 1, according to one embodiment of the invention. FIGS. 8A-8C shows an administrator dashboard screen that includes general operating information regarding the 3D printer management 100. As shown in FIG. 8A, the administrator dashboard screen contains high-level information regarding the database integrity, management server information, active objects (including 3D printers and authorized users) in the 3D printer management network 100, and any printing jobs that were canceled as a result of a system restart. As shown in FIG. 8B, the administrator dashboard screen further contains shortcuts to various system settings, including email settings, language settings, regional settings, user settings, device settings, payment settings, and print job parser settings. Finally, as shown in FIG. 8C, the administrator dashboard screen also includes high-level status information regarding system services and locks on devices.

[0068] FIG. 8D shows a reports screen providing a report of the print requests received from authorized users. The reports screen includes information regarding the print request, including the user's identification, the device the print request originated from, the status of the print request (accepted, printed, deleted, printer error, etc.), the time the request was made, and the type of printing requested. FIG. 8E shows a summary screen

of a user's print request. As shown in FIG. 8E, the summary screen includes basic information including the file name and the owner of the file, information about the 3D model to be printed, including the estimated time it will take to print the model and the amount of material required, information regarding the status of the print job, and the identification numbers of the print job and management server.

[0069] FIG. 8F shows a devices screen indicating the 3F printers currently connected to the 3D printing network 100. As shown in FIG. 8F, six 3D printers are currently connected to the network. From the devices screen of FIG. 8F, an administrator may also add new 3D printers to the 3D printing network 100 and group 3D printer devices together. FIG. 8G shows a billing screen with price lists for 3D printing requests. As shown in FIG. 8G, an administrator has created a custom price list entitled "eDee." Additionally, a default price list is available.

[0070] Price lists may be automatically calculated based on measured parameters (including type of material used, amount of material used, time, number of previous print requests, complexity of the 3D model, etc.). Additionally, statistics and analysis may be prepared for an administrator to help the administrator set custom price lists. In one embodiment, the administrator may apply different price lists to different 3D printers within the 3D printer network. In another embodiment, the administrator may apply different price lists to different users. From the price list screen of FIG. 8G, an administrator may also create a new price list and edit existing price lists. In one embodiment, changes to the price list may be automatically recommended to the administrator based on the specific circumstances of the 3D printing network 100. For

example, the administrator may be recommended to increase the price list by 10% in order to ensure the 3D printer management network 100 is not being operated at a loss.

[0071] FIG. 8H shows a payment account screen summarizing the account balances of authorized users. From the payment account screen shown in FIG. 8H, an administrator may select and view the transaction history of each user, update the user's account balance, issue refunds, and set up periodic balance recharging for a user account, whereby the user's account is credited a specified amount every designated period. FIG. 8I shows a transaction history screen of a user. As shown in FIG. 8I, the transaction history of each user, including the transaction type, the amount charged, any taxes charged, and the details of the print job (including the transaction id) can be viewed by the administrator.

[0072] FIG. 8J shows a user account list screen identifying the authorized users of the 3D printer management network 100. As shown in FIG. 8J, there are three currently authorized users, however, the number of users that may be supported by the 3D printer management network 100 may be significantly greater than the number shown in FIG. 8J. Additional information about each user, including their name and email address is also displayed on the user account list screen. From the user account list screen shown in FIG. 8J, an administrator may modify a user's access rights within the 3D printer management network 100.

[0073] FIG. 8K shows a user's access rights screen for a user. As shown in FIG. 8K, an administrator has broad control over the access rights to the various features of the 3D printer management network 100, from access and control of the user's own account, to print job reports, and so on and so forth. In this manner, an administrator has full

controller over what an authorized user can and cannot do within the 3D printer management network 100. An administrator may specify the access rights to each individual user, given an administrator full control and flexibility over each user's access rights.

[0074] Other objects, advantages and embodiments of the various aspects of the present invention will be apparent to those who are skilled in the field of the invention and are within the scope of the description and the accompanying Figures. For example, but without limitation, structural or functional elements might be rearranged, or method steps reordered, consistent with the present invention. Similarly, principles according to the present invention could be applied to other examples, which, even if not specifically described here in detail, would nevertheless be within the scope of the present invention. For example, the principles of the present invention are not limited to 3D printing, and can be equally applicable to any type of additive or subtractive manufacturing devices.

What is claimed is:

1. A printer management system comprising:

one or more printing devices comprising

a printing area for printing according to a digital file;

an access area through which a user may access the printing area;

a locking mechanism configured to lock the access area preventing the user from accessing the printing area; and

a management server communicatively coupled to each of the one or more printing devices over a communications network,

wherein the management server is configured to

receive a print request from one or more user devices or one of the one or more printing devices to print the digital file,

transmit the digital file to a selected one of the one or more printing devices, and

transmit commands to lock and unlock the locking mechanism of the one or more printing devices.

2. The printer management system of claim 1, wherein the one or more printing devices are configured to lock the locking mechanism during printing of the digital file, and unlock the locking mechanism upon receiving a command from the management server or from an authorized user or upon an authorized user manually unlocking the locking mechanism.

3. The printer management system of claim 1, wherein the management server is further configured to update a printing status of each of the one or more printing

devices and the selected one or more printing devices is selected based upon the printing status of each of the one or more printing devices.

4. The printer management system of claim 1, wherein the one or more printing devices further comprises a user interface,

wherein the user interface is configured to

authenticate an authorized user, and

unlock the locking mechanism in response to an unlock command from the authorized user.

5. The printer management system of claim 1, wherein the locking mechanism comprises an electromagnetic lock.

6. The printer management system of claim 1, wherein the locking mechanism comprises a mechanical bolt-action lock.

7. The printer management system of claim 4, wherein the management server is further configured to store a plurality of digital files, and the user interface is further configured to retrieve, in response to a request from the authorized user, a selected one or more digital files of the plurality of digital files for printing by the printing device.

8. The printer management system of claim 4, wherein the user interface is further configured to transmit, in response to a print command from the authorized user, the print request to the management server.

9. The printer management system of claim 1, wherein the print request comprises the metadata for the digital file.

10. The printer management system of claim 9, wherein the metadata comprises at least one of a file name of the digital file, an owner of the digital file, an estimated time to print the digital file, and an estimated amount of material required to print the digital file.

11. The printer management system of claim 3, wherein the printing status indicates printer operation time, printer occupation time, or printer material remaining.

12. The printer management system of claim 1, wherein the one or more printing devices further comprises a moveable panel adapted to cover the access area when disposed in a closed position, wherein the locking mechanism is configured to lock the moveable panel in the closed position.

13. A printer management system comprising:

a management server capable of being communicatively coupled to one or more printing devices over a communications network,

wherein, the management server is configured to

receive, over the communications network, a print request from one or more user devices or the one or more printing devices to print a digital file,

transmit, over the communications network, the digital file to a selected one or more printing devices, and

transmit, over the communications network, commands to lock and unlock a locking mechanism of the one or more printing devices, the locking

mechanism configured to secure an access area through which a user may access a printing area of the printing device for printing the digital file.

14. The printer management system of claim 13, wherein the management server transmits the command to lock the locking mechanism of the selected one or more printing devices prior to printing of the digital file, and transmits the command to unlock the locking mechanism of the selected one or more printing devices at a time after the digital file has completed printing.

15. The printer management system of claim 13, wherein the management server is further configured to update a printing status of each of the one or more printing devices.

16. The printer management system of claim 13, wherein the management server is further configured to store the digital files received from the one or more user devices.

17. The printer management system of claim 13, wherein the print request comprises the metadata for the digital file.

18. The printer management system of claim 17, wherein the metadata comprises at least one of a file name of the digital file, an owner of the digital file, an estimated time to print the digital file, and an estimated amount of material required to print the digital file.

19. The printer management system of claim 15, wherein the printing status indicates printer operation time, printer occupation time, or printer material remaining.

20. A printing device comprising:

a printing area for printing a digital file;

an access area through which a user may access the printing area; and

a locking mechanism configured to lock the access area preventing the user from accessing the printing area,

wherein

the printing device is capable of being communicatively coupled to a management server, and

the printing device is configured to lock the locking mechanism during printing of the digital file, and unlock the locking mechanism upon receiving a command from an authorized user or from the management server.

21. The printing device of claim 20, wherein the locking mechanism comprises an electromagnetic lock.

22. The printing device of claim 20, wherein the locking mechanism comprises a mechanical bolt-action lock.

23. The printing device of claim 20, further comprising:

a user interface,

wherein the user interface is configured to

authenticate an authorized user, and

unlock the locking mechanism in response to an unlock command from the authorized user.

24. The printing device of claim 20, further comprising a moveable panel adapted to cover the access area when disposed in a closed position, wherein the locking mechanism is configured to lock the moveable panel in the closed position.

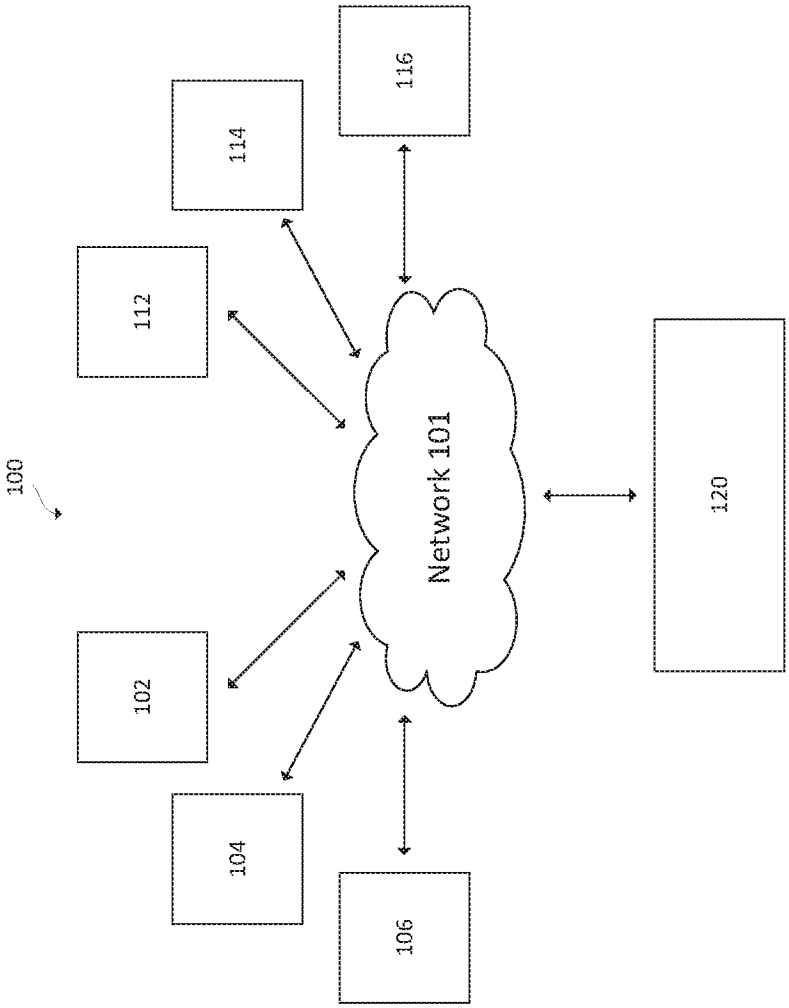


FIG. 1

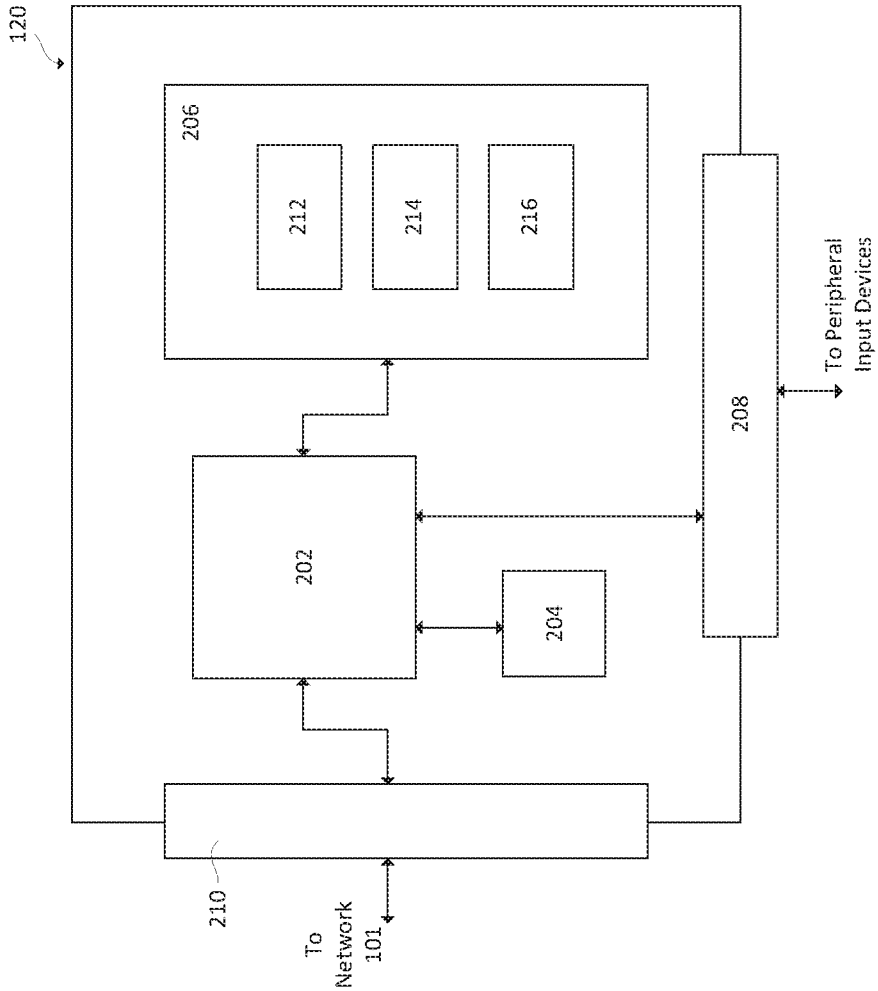

120
206
212
214
216
202
204
208
To Peripheral Input Devices 201
210
To Network 101

FIG. 2

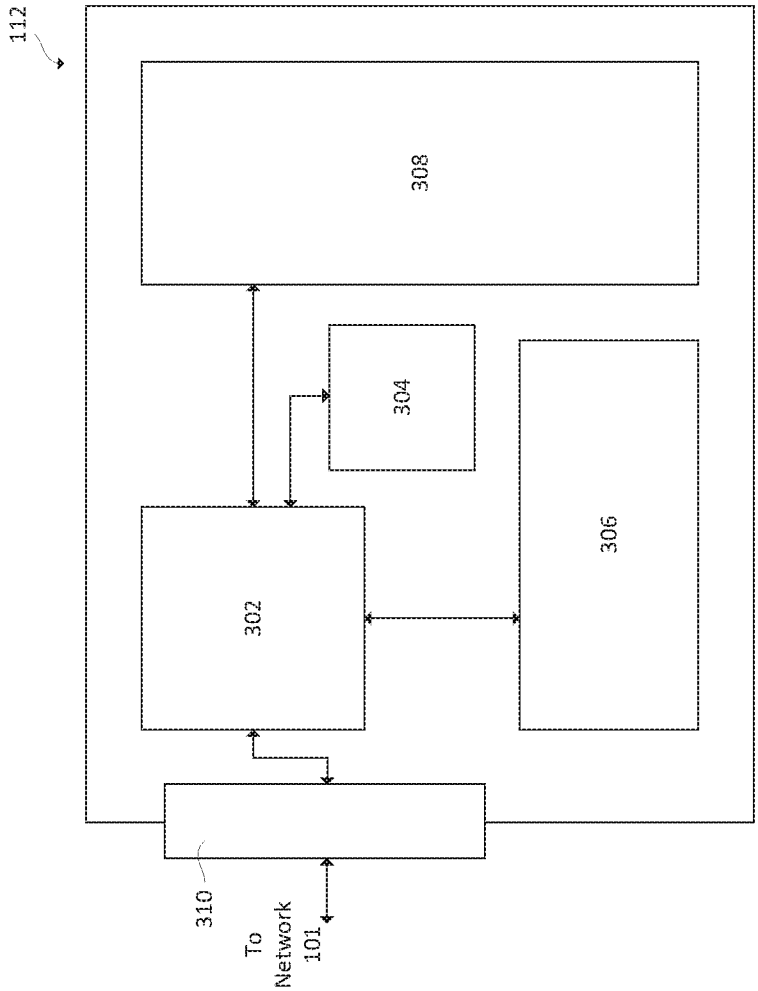


FIG. 3

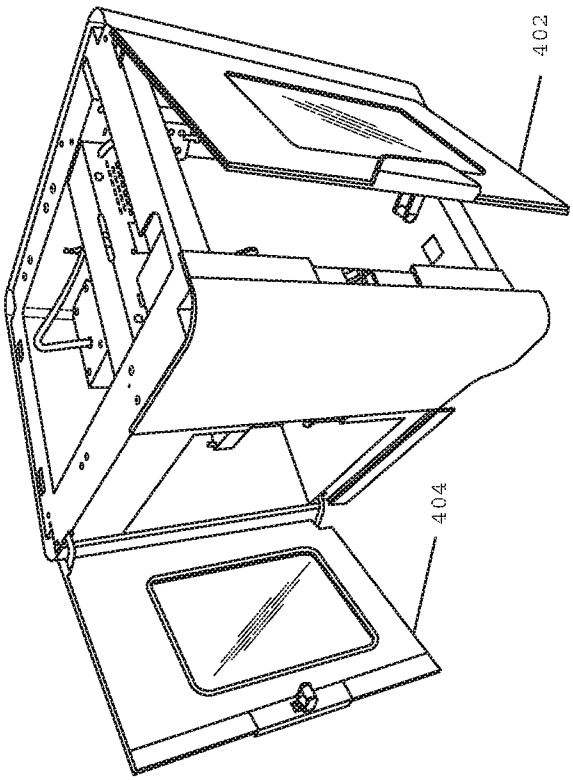


FIG. 4A

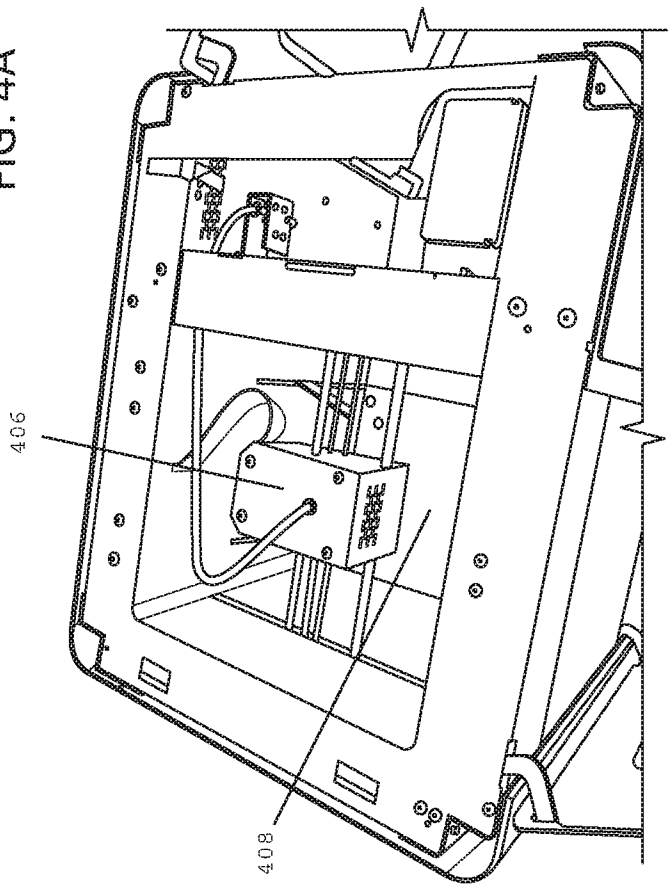


FIG. 4B

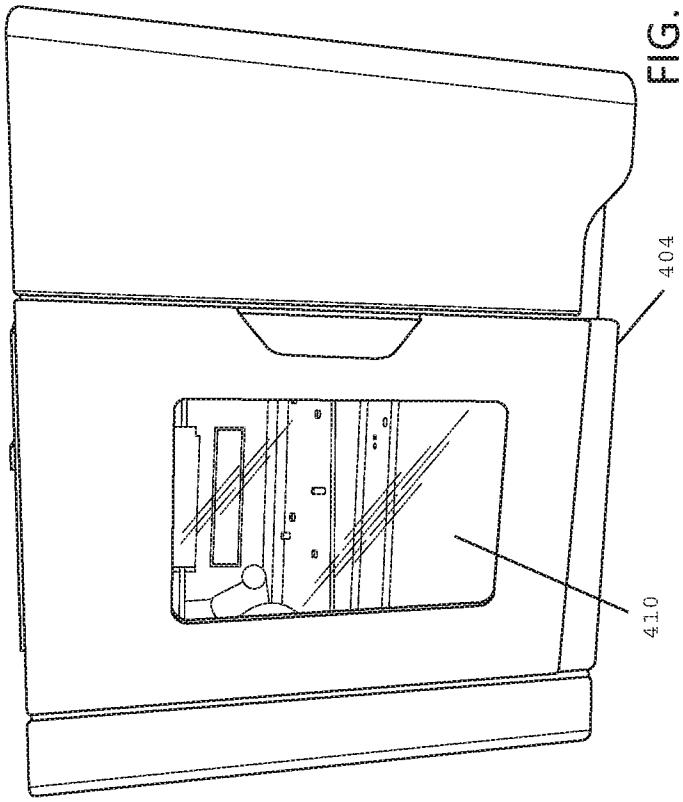


FIG. 4C

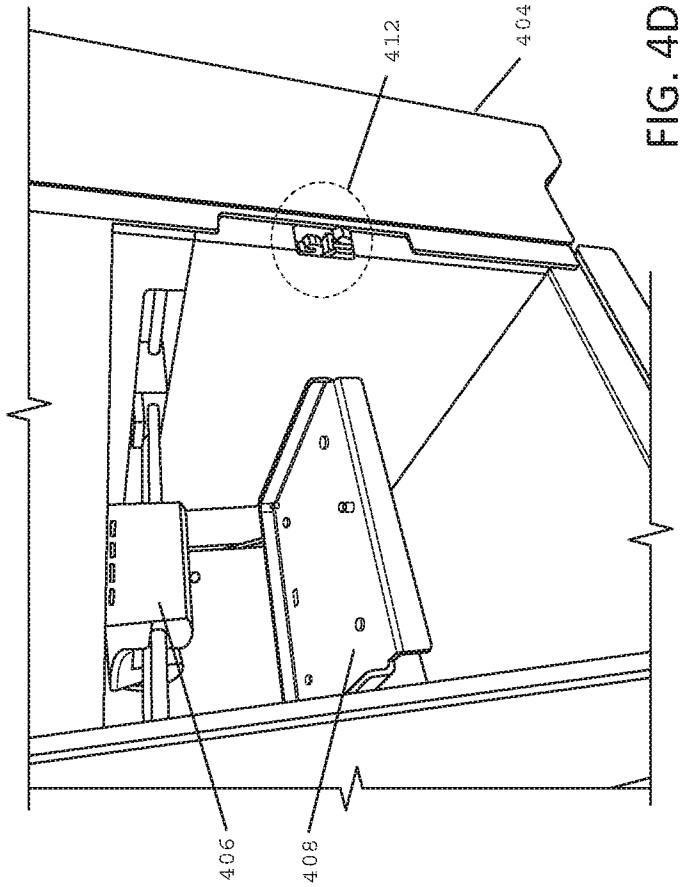


FIG. 4D

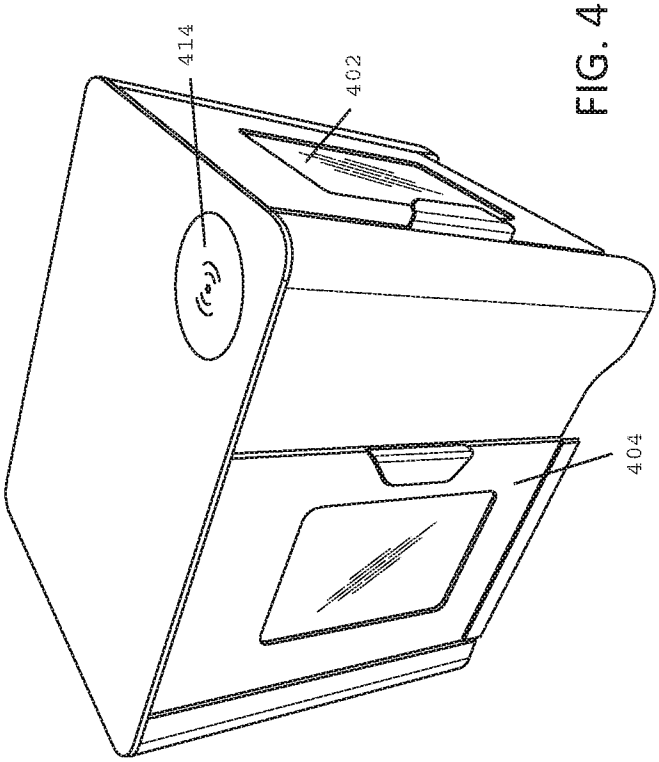


FIG. 4E

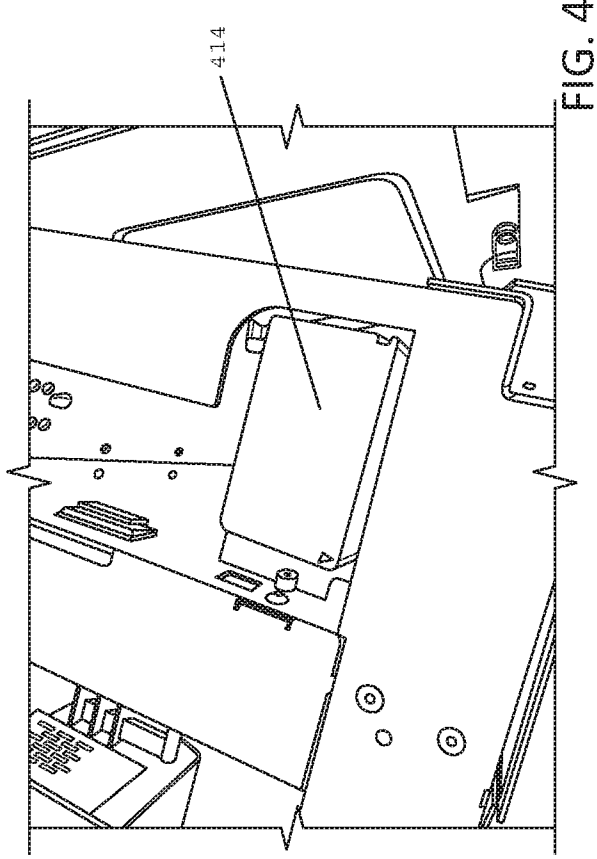


FIG. 4F

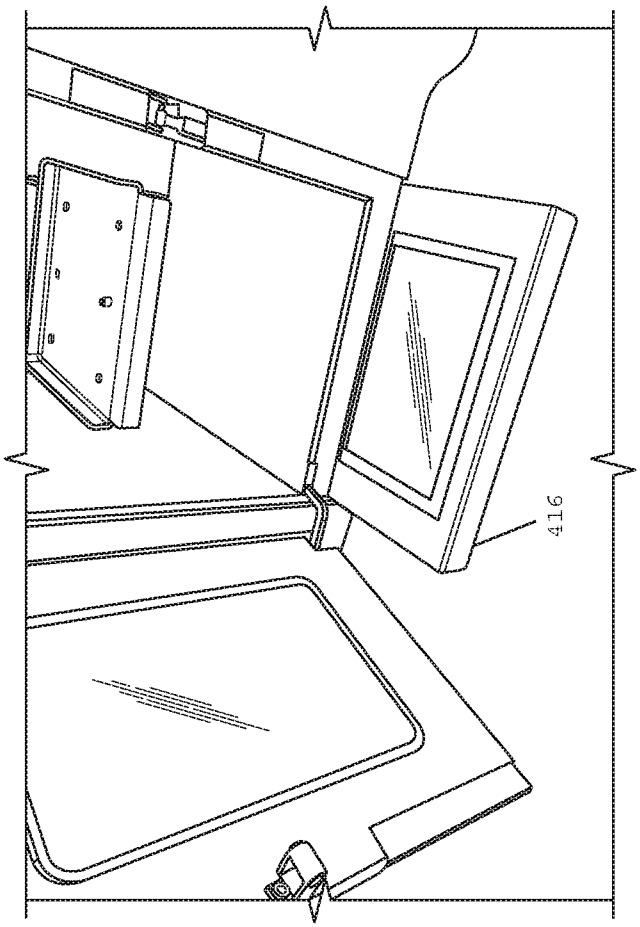


FIG. 4G

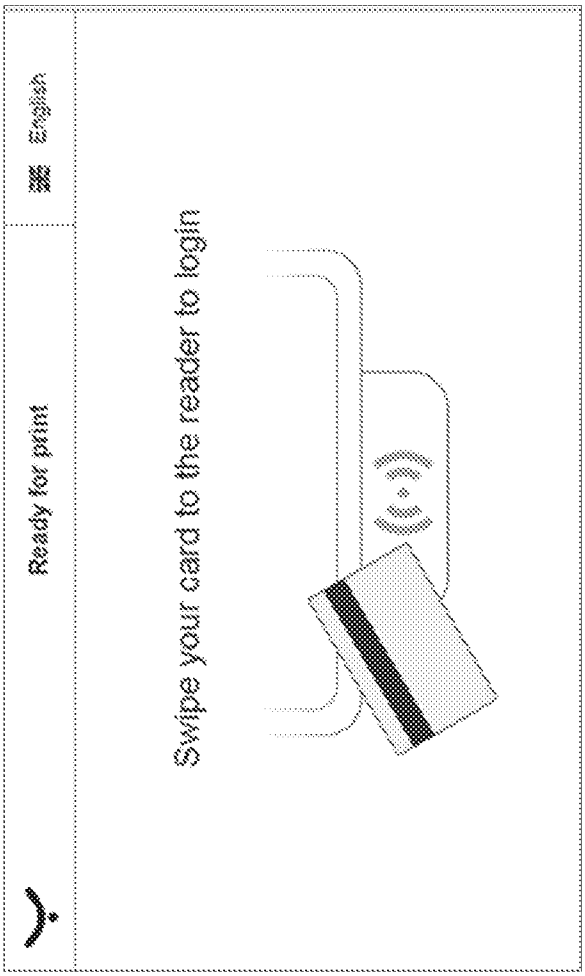

Ready for print
English
Swipe your card to the reader to login

FIG. 5A

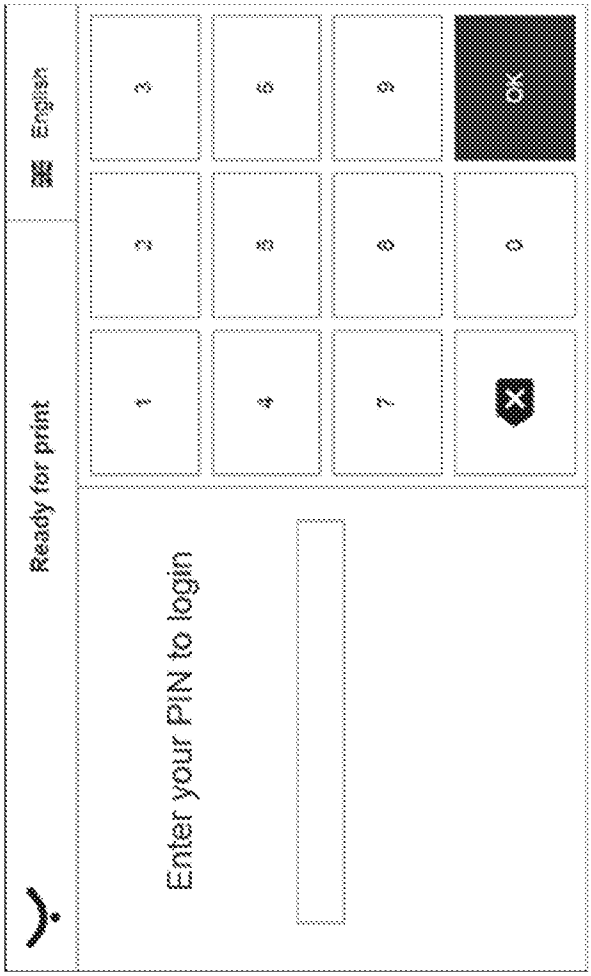

Ready for print
English
Enter your PIN to login
1
2
3
4
5
6
7
8
9
0
OK

FIG. 5B

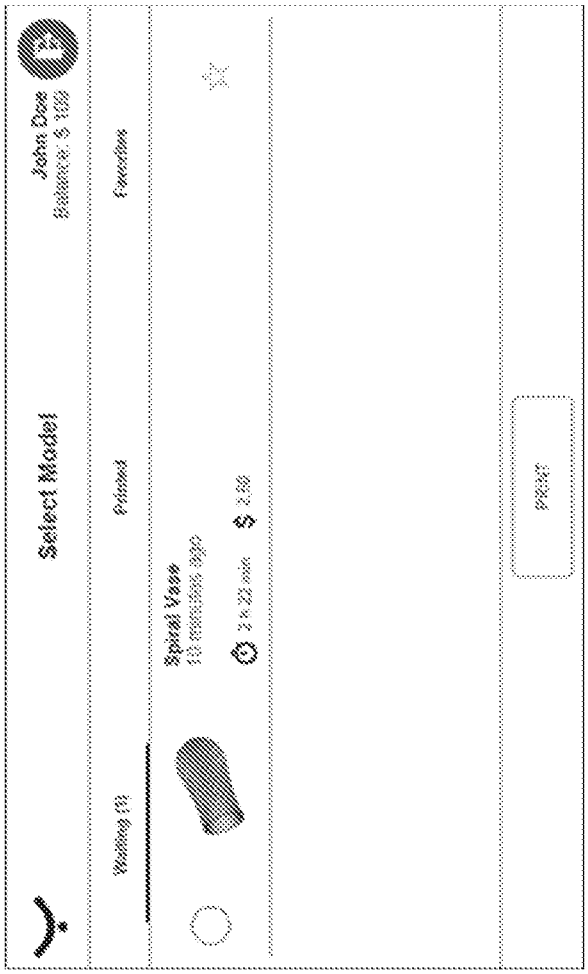

Select Model
John Doe
Balance: $ 100
Printed
Favorites
Spiral Vase
PRINT

FIG. 5C

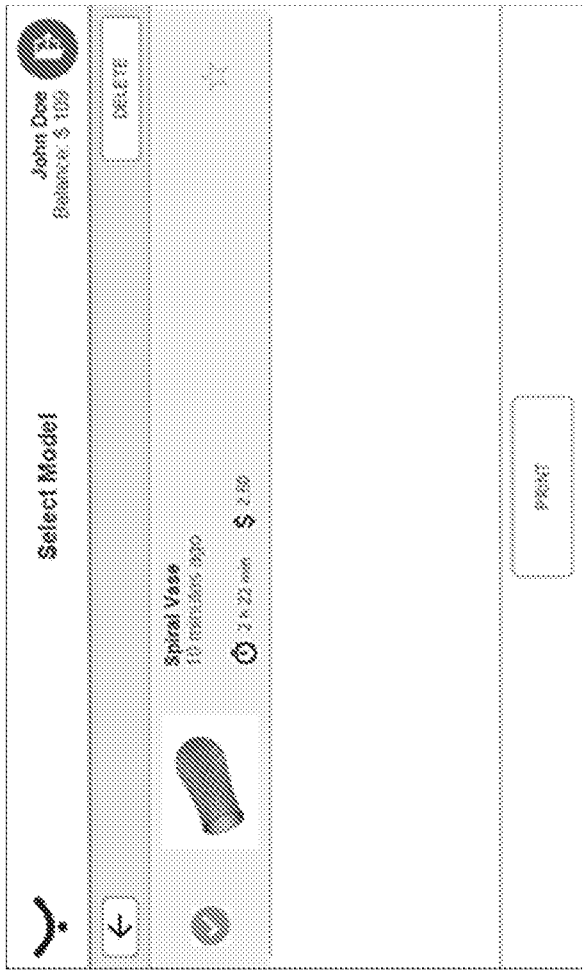

Select Model
John Doe
Balance: $ 100
DELETE
Spiral Vase
PRINT

FIG. 5D

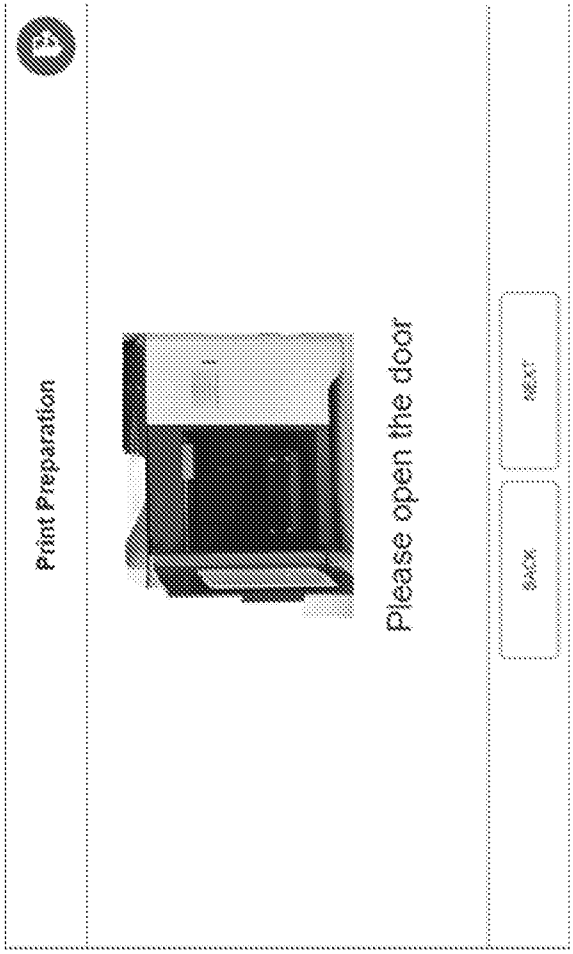

Print Preparation
Please open the door
BACK
NEXT

FIG. 5E

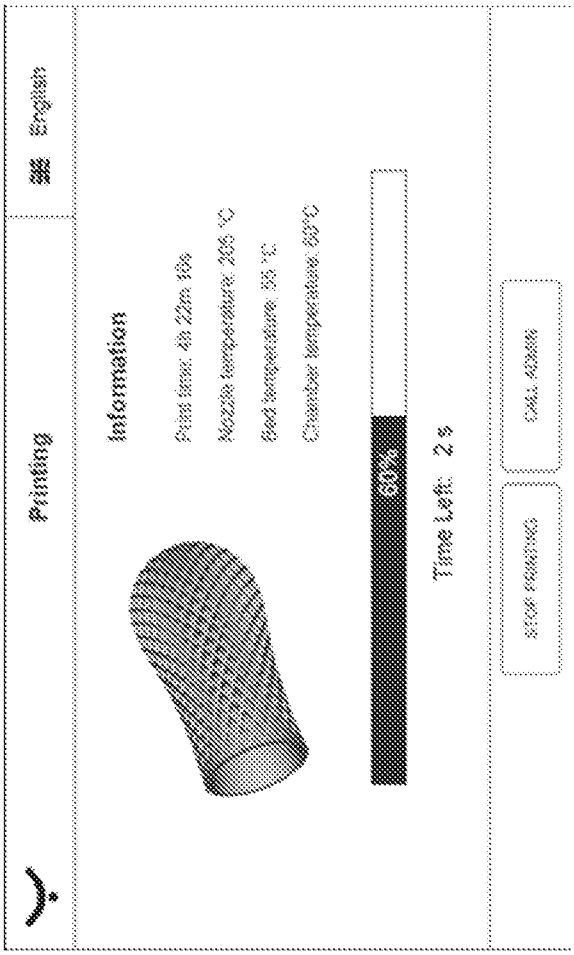

Printing
English
Information
Print time: 4h 22m 16s
Nozzle temperature: 205 °C
Bed temperature: 55 °C
Chamber temperature: 60°C
60%
Time Left: 2s
STOP PRINTING
CAL 40MM

FIG. 5F

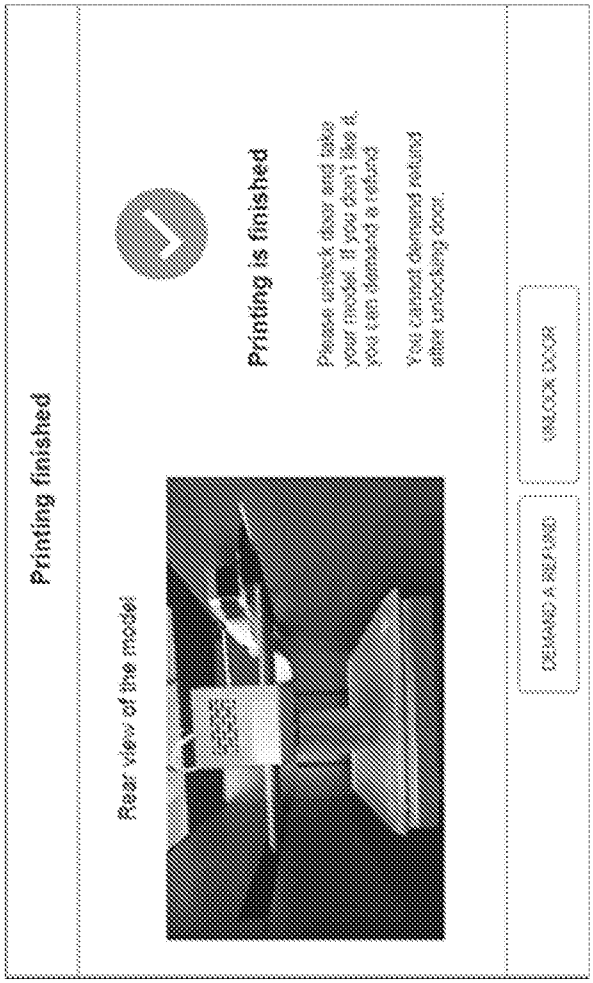

Printing finished
Rear view of the model
Printing is finished
Please unlock door and take your model. If you don't like it, you can demand a refund.
You cannot demand refund after unlocking door.
DEMAND A REFUND
UNLOCK DOOR

FIG. 5G

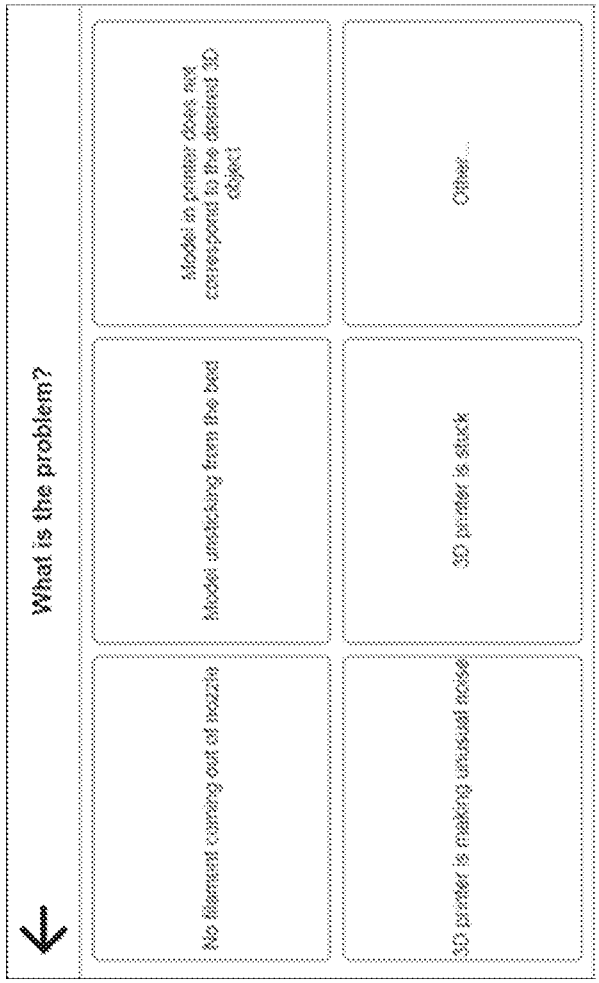

What is the problem?
No filament coming out of nozzle
Model not sticking from the bed
3D printer is making unusual noise
3D printer is stuck
Model in printer does not correspond to the desired 3D object
Other...

FIG. 5H

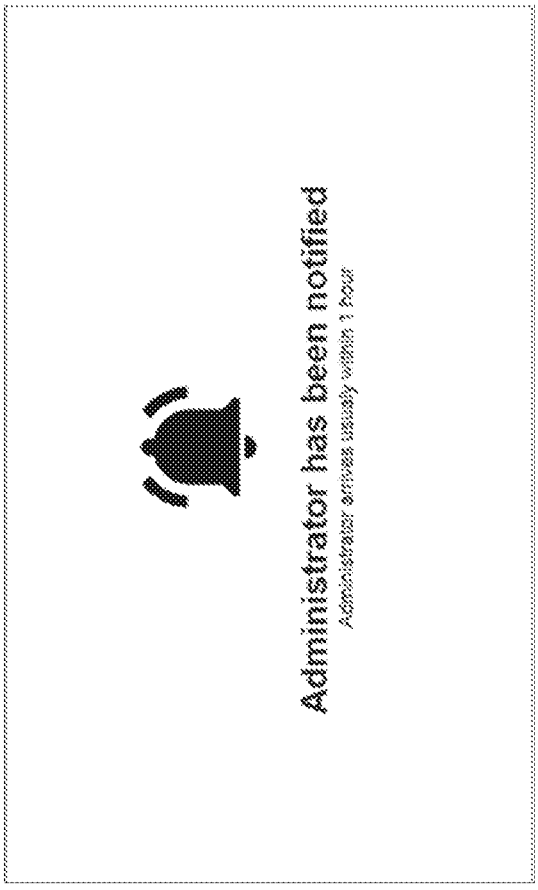

Administrator has been notified
Administrator arrives usually within 1 hour

FIG. 5I

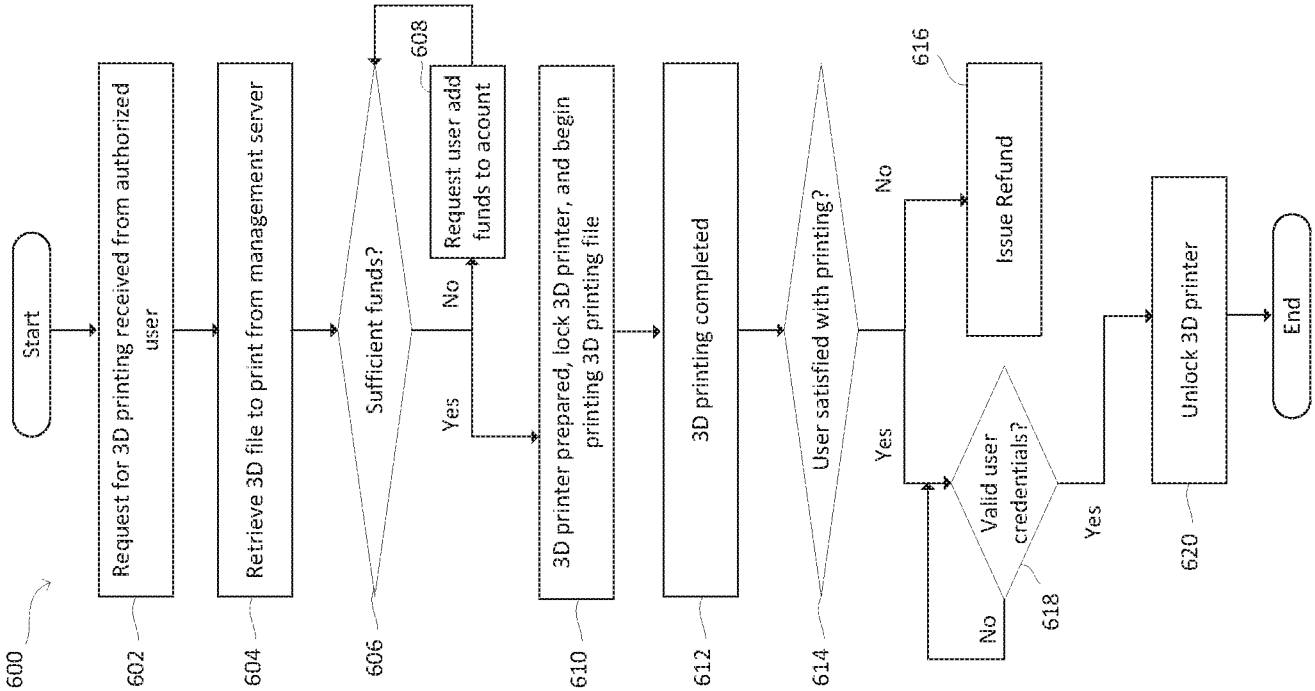

Start
Request for 3D printing received from authorized user
Retrieve 3D file to print from management server
Sufficient funds?
No
Request user add funds to acount
Yes
3D printer prepared, lock 3D printer, and begin printing 3D printing file
3D printing completed
User satisfied with printing?
No
Issue Refund
Yes
Valid user credentials?
No
Yes
Unlock 3D printer
End
600
602
604
606
608
610
612
614
616
618
620

FIG. 6

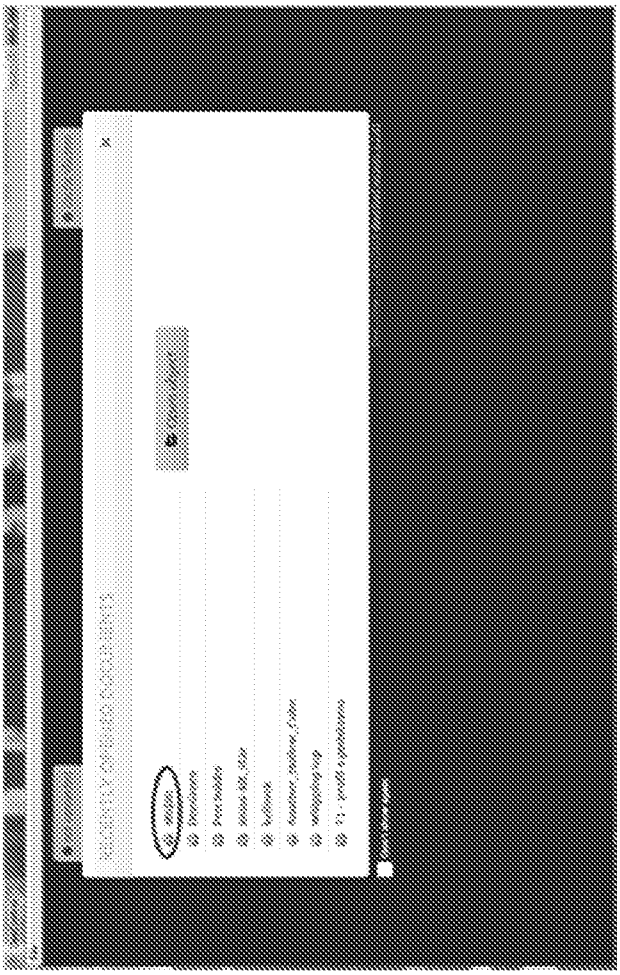


FIG. 7A

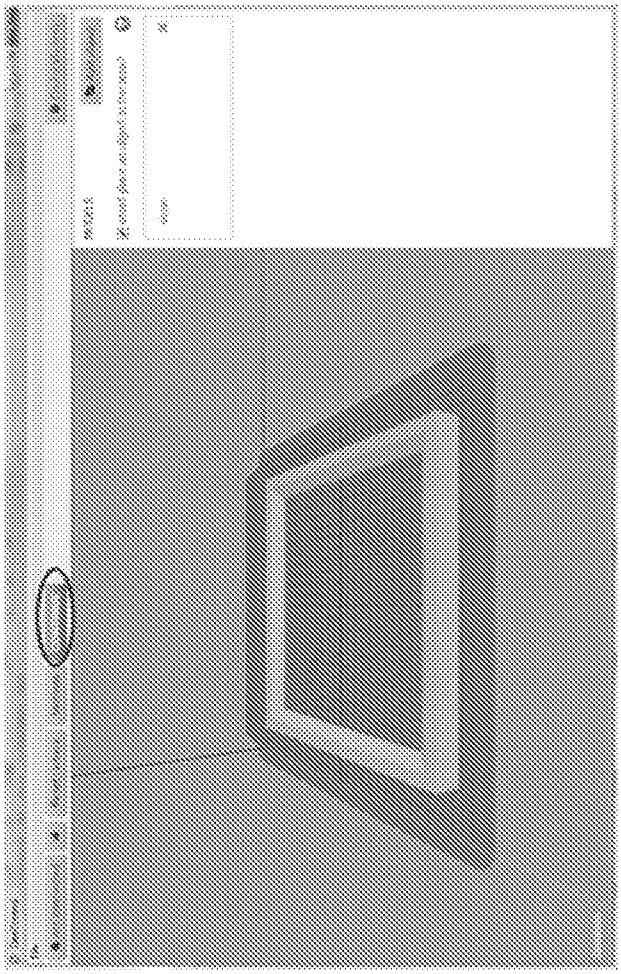


FIG. 7B

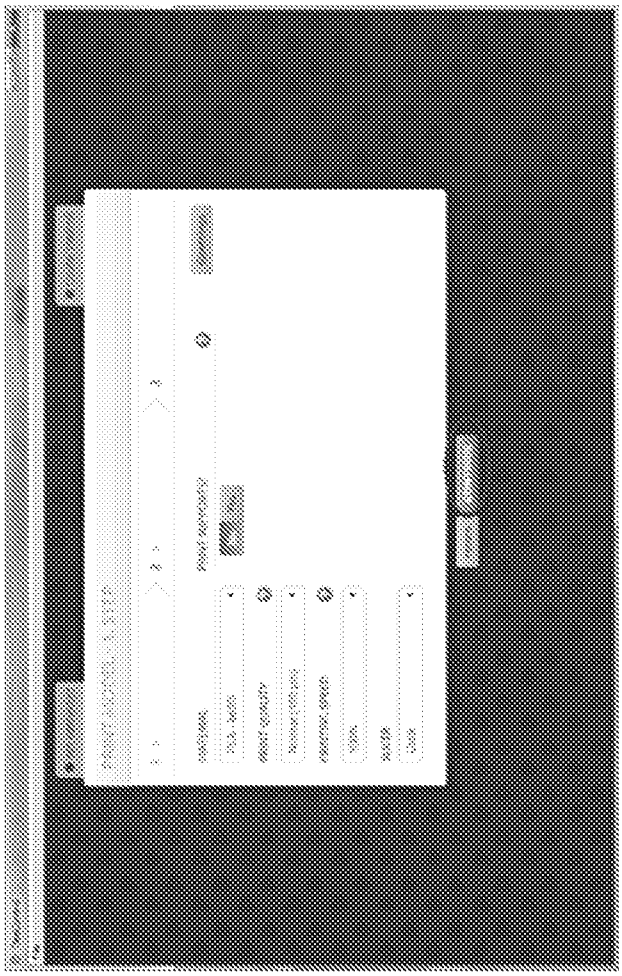


FIG. 7C

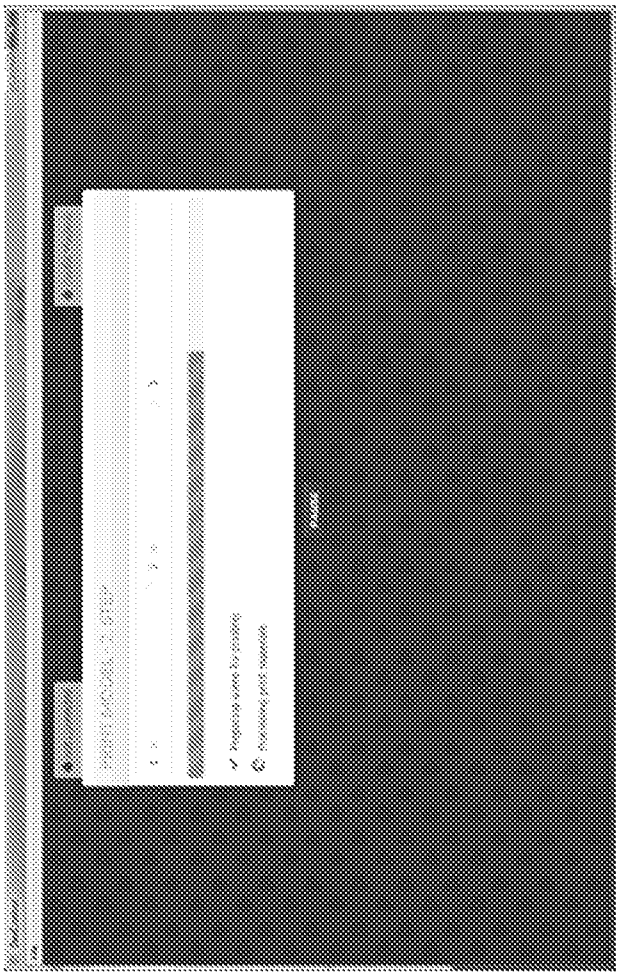


FIG. 7D

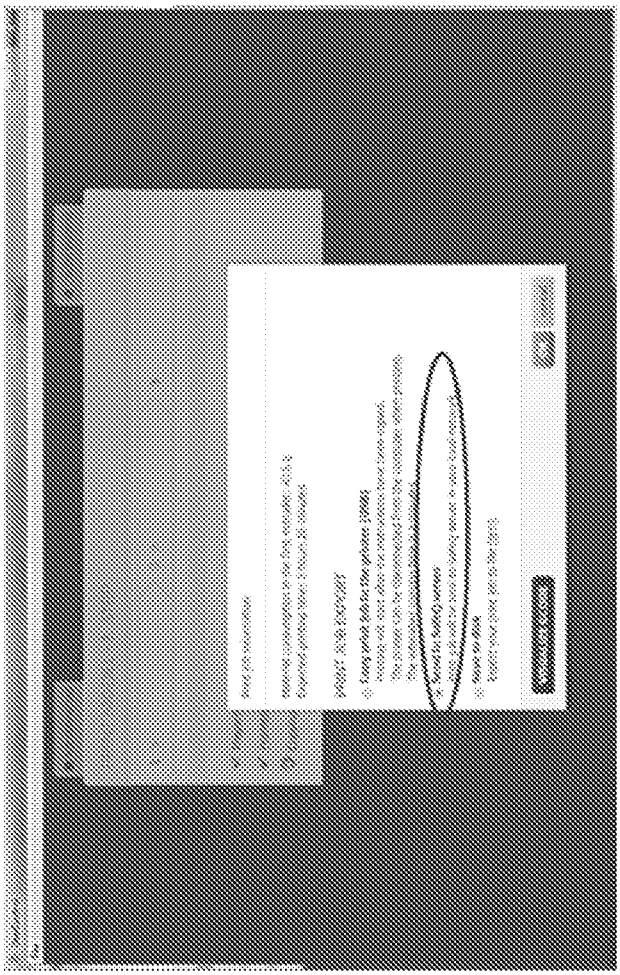


FIG. 7E

Dashboard
Dashboard > Dashboard
Tenant Management
tenant_1
SafeQAdministrator
admin
Dashboard
Jobs
Devices
Users
Print
Components
Users
Quotas
System
Dashboard
Customize
YSoft SafeQ version
YSoft SafeQ 6 SR
Internal build
8.6.0.001
Support ID
RA11000001
Customer
client_on_0A10-8203-10.6.10.33
License expiration
24.1.2016
Support expiration
24.12.2015
License information
Support information
About the YSoft SafeQ application
Database integrity
Usernames, aliases
OK
User, cost center, and role links
OK
User cards
OK
Devices network addresses
OK
Terminal serial numbers
OK
Local printers
OK
Last update: 11.10.16 Next update: 14.10.16
System info
Server uptime
14 Wk 1 Wkm, 5 Mon, 0 Mi
CML GMB
CML 1
Windows Server 2008 R2 on GA13S018 (model Family 6 Model 26 Stepping 4, GenuineIntel, 2x2GHz)
Operating system and configuration
Active objects in system
Devices
11
Users
0
Hardware terminals
0
Cost centers
1
Embedded terminals
0
Roles
7
OIDs
0
Billing codes
1
Last update: 11.10.16 Next update: 14.10.16
Jobs canceled by system restart
Jobs that were being processed during YSoft SafeQ shutdown have been automatically canceled. Click the Find automatically canceled jobs button to locate such jobs. You have the option to cancel them permanently or to requeue them for immediate processing.
Locating the canceled jobs may take several minutes.
Welcome to YSoft SafeQ
You must set up these items before you start using YSoft SafeQ.

FIG. 8A

Dashboard
Tenants
Printers
Terminals
Users
Payments
Print jobs
System
Dashboard › Dashboard
Tenant Management
tenant_1
SafeQAdministrator
admin
Dashboard
Email settings
Language settings
Regional settings
Users, card centers, and roles
Devices
Ycash Payment System
Print job parser
System is ready
Server load (ONLY from OKS servers) 0.00
Database structure OK
2.0 SP2
(2.0.50727.5420)
3.0 (3.0.30729.5420)
3.5 SP1
(3.5.30729.5420)
4.0 Client Profile
(4.5.51209)
4.0 Full Profile
(4.5.51209)
.NET version
Find automatically cancelled jobs
Text encryption
Enter text to encrypt:
ENCODE
More details
Printed/failed jobs
No data have been recorded since YSoft SafeQ server started.
System services
SQL Listener (OSK)
Communicator
Enterprise Server Synchronization
Stopped
Running
Running

FIG. 8B

Dashboard
Dashboard
Tenant Management
Tenant_1
SafeQAdministrator
Admin
Dashboard
System services
SSL Listener (CSD)
Stopped
Communication
Running
Enterprise Server Synchronization
Running
CSD Synchronization
Stopped
UWP Application Service
Running
Watch Payment System
Running
Locks on devices
All locks are found (MASTER server node is selected).
Number of locks held on CMS servers:
Number of CMS servers that are holding locks:
Dashboard
Devices
Clients
Users
Payments
Users
Clients
System

FIG. 8C

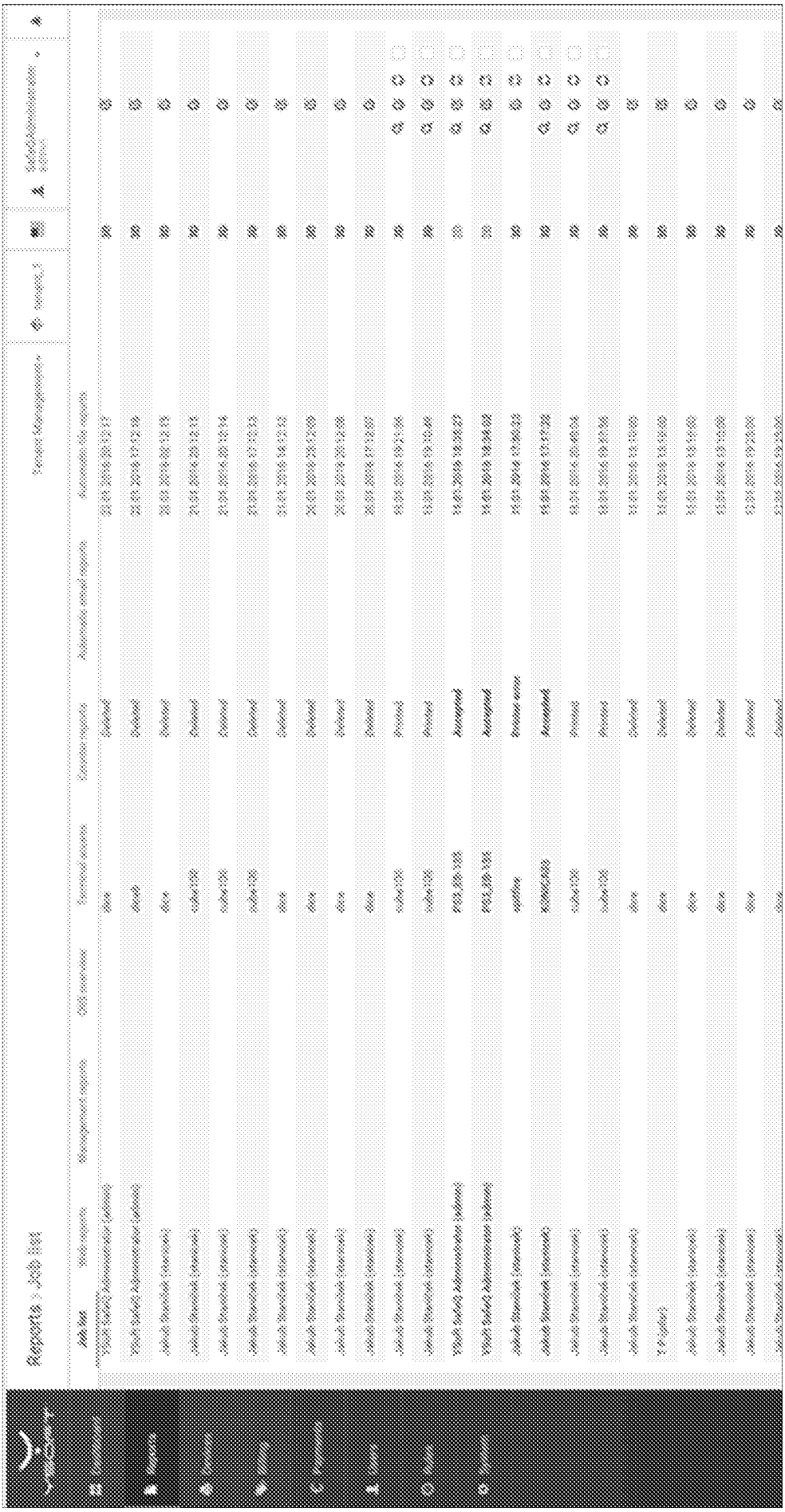


FIG. 8D

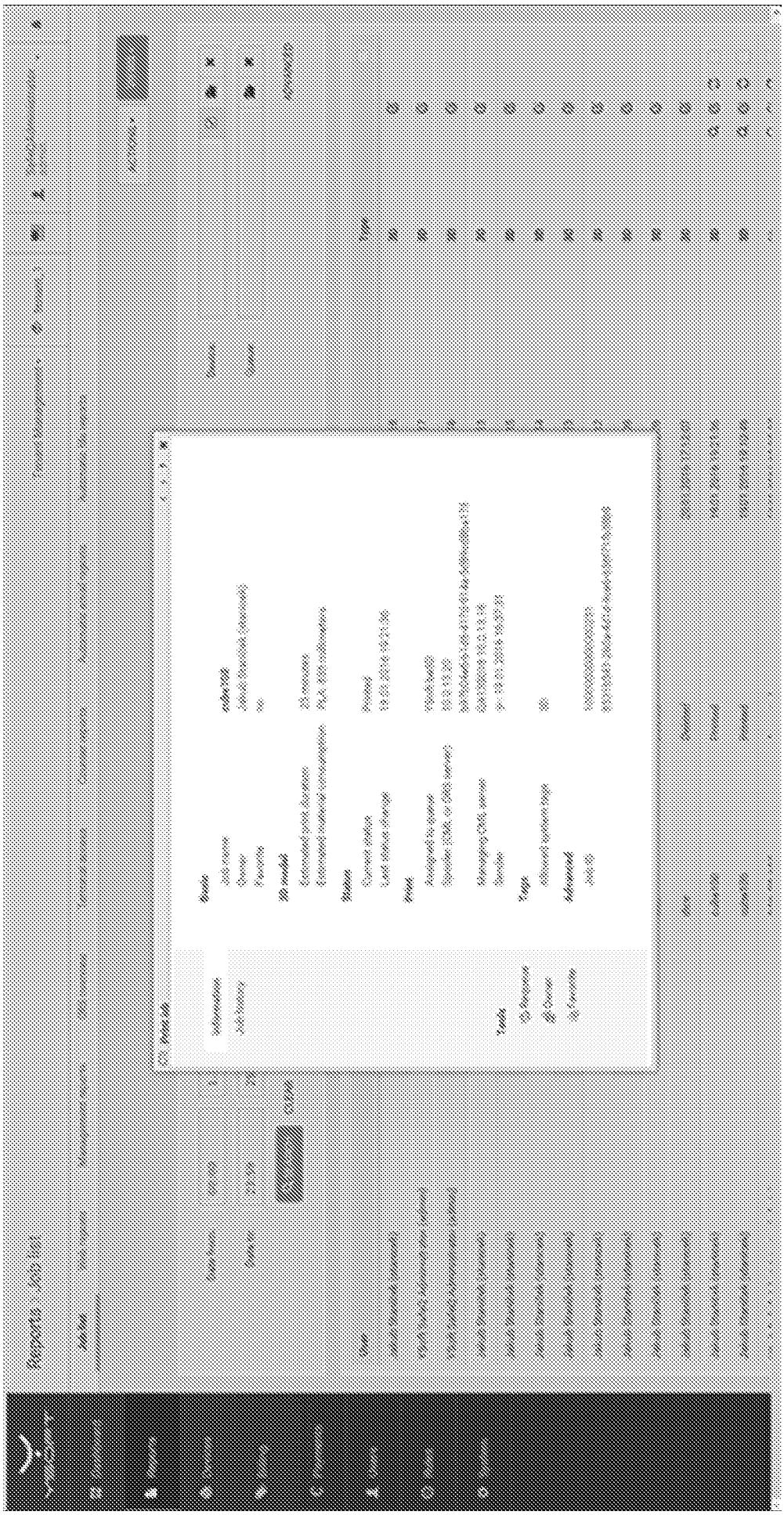


FIG. 8E



FIG. 8F

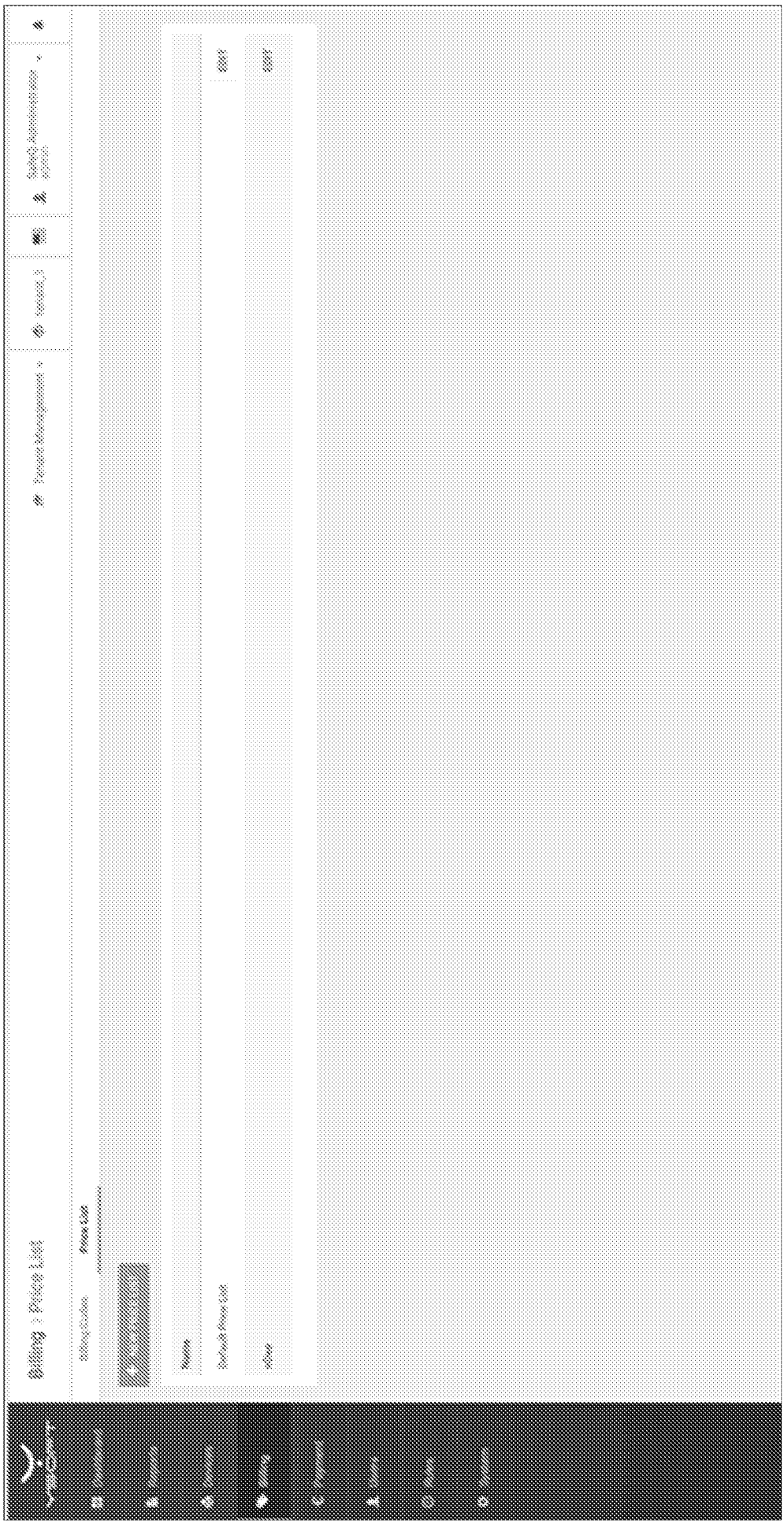


FIG. 8G

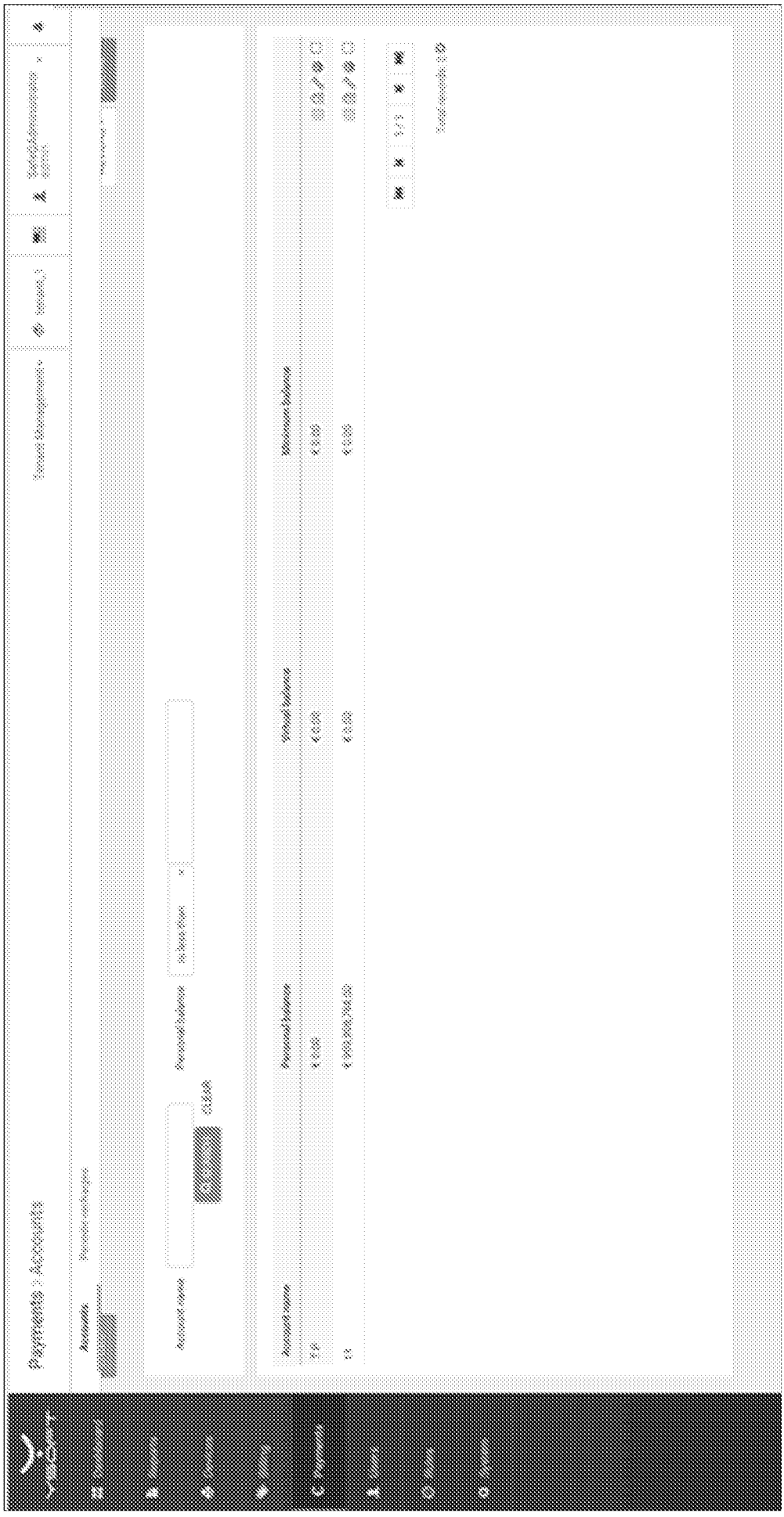


FIG. 8H

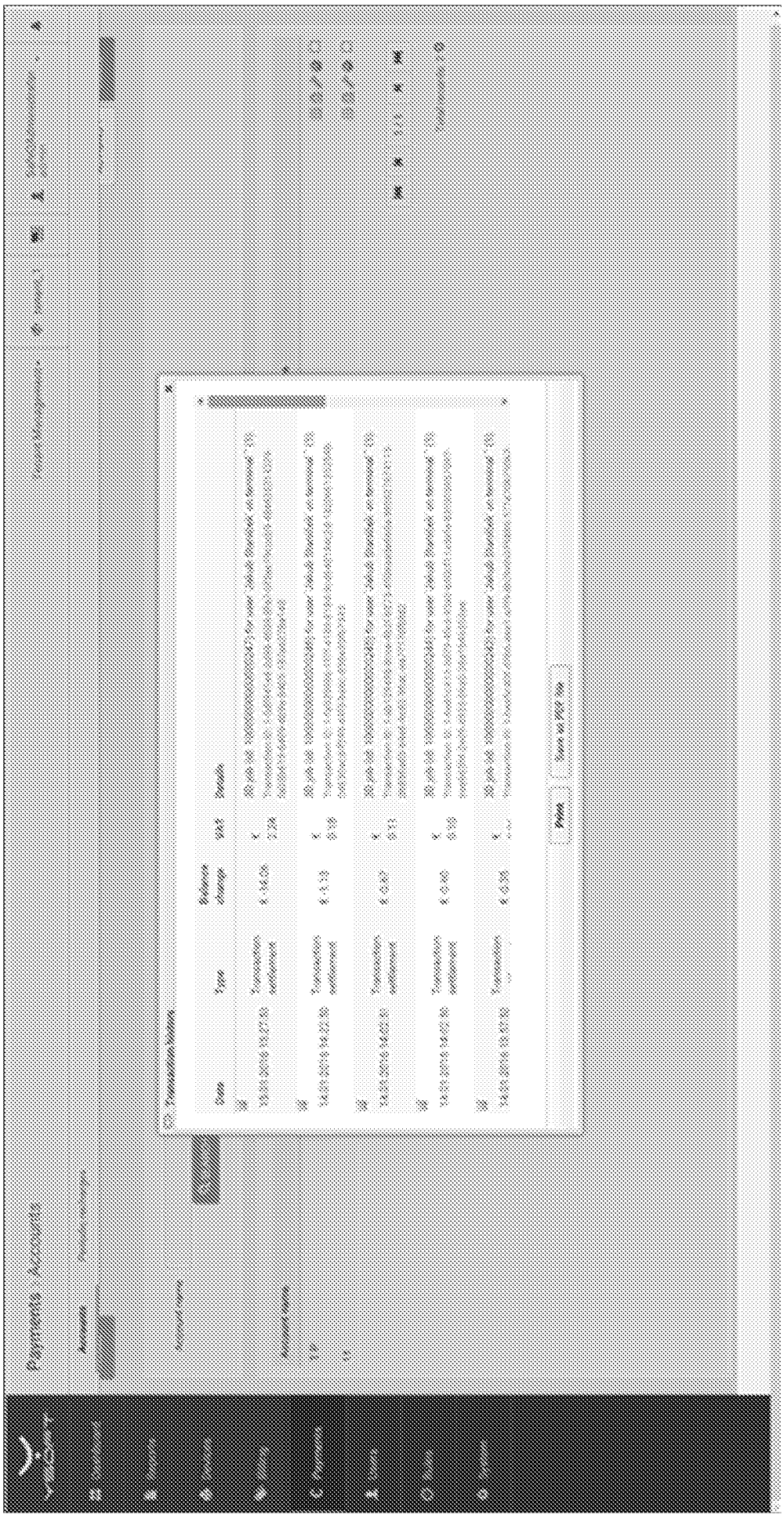


FIG. 8I

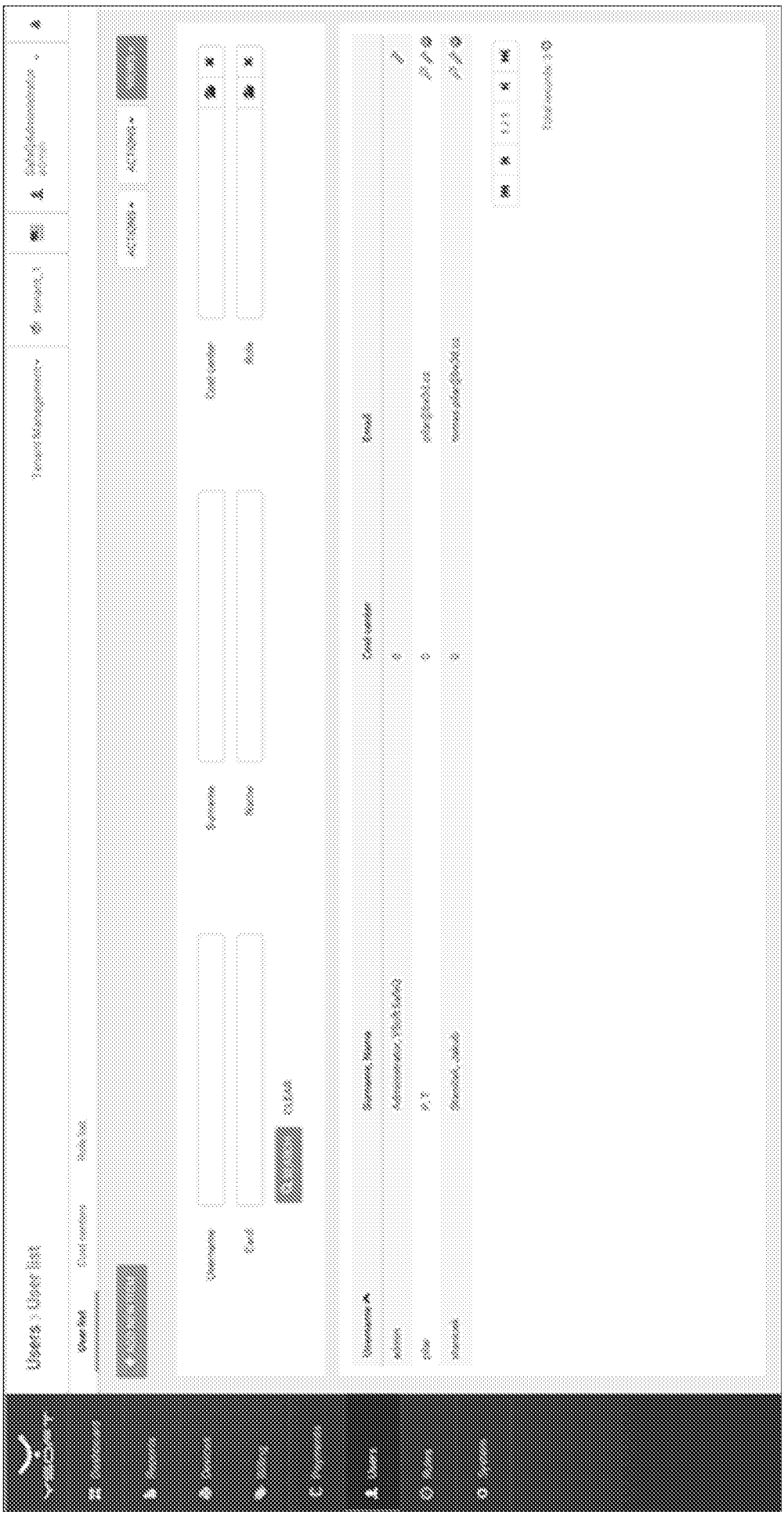


FIG. 8J



FIG. 8K

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/000130

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N1/44 B33Y30/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B29C H04N B33Y

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/288699 A1 (WILLIAMS CHRISTOPHER B [US] ET AL) 25 September 2014 (2014-09-25) the whole document	1-24
X	US 2015/197064 A1 (WALKER CHRISTOPHER [US] ET AL) 16 July 2015 (2015-07-16) paragraphs [0004] - [0135]	1-24
A	US 2015/082372 A1 (KOTTAHACHCHI BUDDHIKA [US] ET AL) 19 March 2015 (2015-03-19) paragraphs [0045], [0082]	1-19
A	US 2014/265046 A1 (BURRIS MATTHEW [US] ET AL) 18 September 2014 (2014-09-18) paragraphs [0022], [0106]	1-24

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 June 2017	19/06/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hardell, Alexander

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2017/000130

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/017393 A1 (STOCKWELL JOHN S [US] ET AL) 27 January 2005 (2005-01-27) paragraph [0047]	1-24
X,P	CN 205 086 360 U (HOU YINGTAO) 16 March 2016 (2016-03-16) the whole document	1,13,20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2017/000130

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014288699 A1	25-09-2014	NONE	
US 2015197064 A1	16-07-2015	NONE	
US 2015082372 A1	19-03-2015	US 2015082372 A1	19-03-2015
		US 2015082373 A1	19-03-2015
		US 2015082396 A1	19-03-2015
US 2014265046 A1	18-09-2014	CA 2900297 A1	18-09-2014
		CN 105188993 A	23-12-2015
		EP 2969320 A1	20-01-2016
		JP 2016522312 A	28-07-2016
		US 2014263209 A1	18-09-2014
		US 2014265046 A1	18-09-2014
		US 2014265047 A1	18-09-2014
		US 2014265048 A1	18-09-2014
		US 2014265049 A1	18-09-2014
		US 2014271328 A1	18-09-2014
		WO 2014144255 A2	18-09-2014
		WO 2014144482 A1	18-09-2014
		WO 2014144630 A1	18-09-2014
US 2005017393 A1	27-01-2005	NONE	
CN 205086360 U	16-03-2016	NONE	