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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 May 2023 (04.05.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/076933 A1

(51) International Patent Classification:
G06Q 20/16 (2012.01) *G06Q 20/10* (2012.01)
G06Q 20/20 (2012.01) *G06Q 20/18* (2012.01)
G06Q 20/38 (2012.01) *G06Q 20/32* (2012.01)
H04L 9/32 (2006.01) *G06Q 20/34* (2012.01)
G06F 21/31 (2013.01) *G06Q 20/40* (2012.01)

(21) International Application Number:
PCT/US2022/078696

(22) International Filing Date:
26 October 2022 (26.10.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/263,089 27 October 2021 (27.10.2021) US

(71) Applicant: **VERIFONE, INC.** [US/US]; 251 Little Falls Drive, Wilmington, Delaware 19808 (US).

(72) Inventors: **GODWIN, David**; 3874 Talah Drive, Palm Harbor, Florida 34684 (US). **HUTZENBILER, Robert J.**; 3610 38th Avenue East, Bradenton, Florida 34208 (US).

(74) Agent: **CAROSA, Daniel R.** et al.; Bond, Schoeneck & King, PLLC, 200 Delaware Avenue, Suite 900, Buffalo, New York 14202-2107 (US).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, 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, ME, 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).

(54) Title: SYSTEMS AND METHODS FOR PAIRING SITE CONTROLLER TO POINT-OF-SALE DEVICES

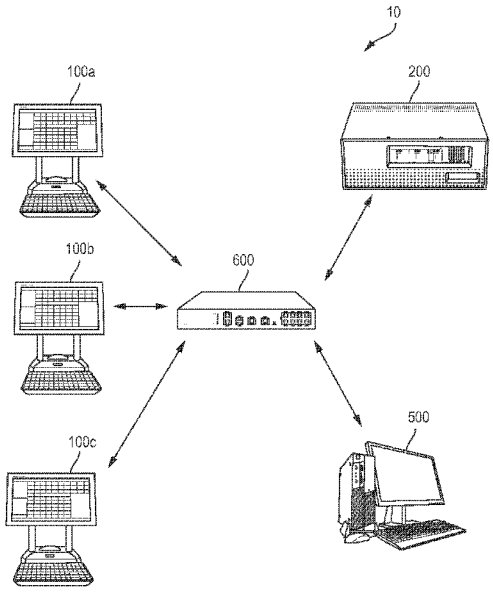


Fig. 1

(57) Abstract: Systems and methods for pairing a point-of-sale device (POS) to a site controller (SC) are provided. The method includes: (1) transmitting, from the POS to the SC, via a legacy communication channel, a start pairing command; (2) generating, via the SC, a one-time password upon receiving the start pairing command; (3) transmitting, via the legacy communication channel, the one-time password from the SC to the POS; (4) transmitting, from the POS to the SC, a host CSR; (5) transmitting, from the SC to the POS, a host certificate, and an SSH-CA public key; (6) transmitting, from the POS to the SC, a user CSR; (7) transmitting, from the SC to the POS, a user certificate; (8) storing, via a memory of the POS, the host certificate, the user certificate, and the SSH-CA public key; and (9) removing keys corresponding to the legacy communication channel from the POS.

WO 2023/076933 A1

[Continued on next page]

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

SYSTEMS AND METHODS FOR PAIRING SITE CONTROLLER TO POINT-OF-SALE DEVICES

Cross-Reference To Related Applications

[0001] This application claims priority to U.S. Provisional Patent Application No. 63/263,089, filed October 27, 2021, and entitled "Systems and Methods for Pairing Site Controller to Point-of-Sale Devices," the entirety of which is incorporated herein by reference.

Field of the Disclosure

[0002] The present disclosure is directed generally to systems and methods for pairing point-of-sale devices to a site controller in retail store environments.

Background

[0003] In-store payment environments may include one or more point-of-sale devices and a site controller. Cashiers utilize the point-of-sale devices to facilitate customer transactions, while the site controller manages the environment by communicating with each point-of-sale device. This communication can involve the site controller issuing commands to one or more of the point-of-sale devices, while also receiving various types of information from the point-of-sale devices. Each point-of-sale device must be paired to the site controller to enable this communication. For security purposes, this pairing is typically a manual process performed by an information technology professional or a similarly skilled and credentialed employee.

[0004] Point-of-sale devices and site controllers often require software upgrades. These software upgrades can be provided automatically to the site controller and point-of-sale devices. The software upgrades are then typically initiated by a store employee outside of normal business hours, such as during the late night and/or early morning. Following installation, the point-of-sale devices must be re-paired to the site controller. However, the store employees initiating the upgrade often lack the technical skills or administrative credentials to perform manual pairing. Failure to pair the point-of-sale devices to the site controller following the software upgrade can effectively disable the point-of-sale devices, leading to significant operational delays and loss of sales. Accordingly, there is a need in the art for an improved process to pair point-of-sale devices to a site controller following a software upgrade.

Summary of the Disclosure

[0005] The present disclosure is generally directed to systems and methods for pairing a site controller to one or more point-of-sale devices. In particular, the systems and methods enable the site controller to pair to the point-of-sale devices as part of an automatic software upgrade. Broadly speaking, the site controller receives a software upgrade. The software upgrade applies to the software of both the site controller and the point-of-sale devices. The site controller and point-of-sale devices were communicatively coupled prior to the initiation of the software upgrade via a legacy communication channel. The site controller first installs the software upgrade pertaining to its own software. The site controller then provides the relevant software upgrades to the point-of-sale devices. The point-of-sale devices install the software upgrades, requiring the point-of-sale devices to be paired with the site controller. The site controller then conveys a one-time password to the point-of-sale devices to pair the site controller to the point-of-sale devices. By automatically pairing the site controller to the point-of-sale devices following the installation of the upgrades, cashiers and other employees may operate the point-of-sale devices without manual pairing, thus reducing downtime.

[0006] However, this automatic pairing is less secure than manual pairing, as the automatic pairing relies on transmitting the one-time password over the legacy communications channel. Transmitting the one-time password over the legacy communications channel can be compromised through a variety of cyber-attacks. Accordingly, in one embodiment, the point-of-sale devices may display a manual pairing reminder window following the automatic pairing. Manual pairing is more secure than automatic pairing, as manual pairing generates new pairing credentials (such as a one-time password). Manual pairing then requires human intervention to retrieve the credentials from the built-in display interface of the site controller (or a corresponding controller client), and to enter the credentials at the point-of-sale device. Thus, a remote attacker would be unable to see the one-time password. Accordingly, manual pairing forms a “trusted relationship” between the point-of-sale device and the site controller.

[0007] This manual pairing reminder window may overlay the functional aspects of the point-of-sale device display interface screen, requiring a cashier to click-through the window to operate the point-of-sale device. The manual pairing reminder window may be configured to be displayed periodically (such as every 5 minutes), or in response to certain actions performed by the point-of-sale device (such as after a completed transaction) until a trusted relationship is established between the point-of-sale device and the site controller via manual pairing. This manual pairing reminder window is meant to remind the cashier to either perform

the manual pairing themselves, or find a skilled and credentialed employee to perform the pairing. Once the manual pairing is performed, the display will no longer show the manual pairing window, as a trusted relationship has been established.

[0008] Generally, in one aspect, a point-of-sale device is provided. The point-of-sale device includes a memory. The memory stores one or more keys corresponding to a legacy communications channel. The point-of-sale device further includes a processor and a transceiver. The point-of-sale device is configured to transmit, via the transceiver over the legacy communication channel, a start pairing command to a site controller. The point-of-sale device is further configured to receive, via the transceiver over the legacy communication channel, a one-time password generated by the site controller. The point-of-sale device is further configured to generate, via the processor, a host certificate signing request (CSR) and a user CSR. The host CSR may be based on the one-time password. The user CSR may also be based on the one-time password. The point-of-sale device is further configured to transmit, via the transceiver, the host CSR and the user CSR to the site controller. The point-of-sale device is further configured to receive, via the transceiver, a host certificate corresponding to the host CSR, a user certificate corresponding to the user CSR, and a secure shell certificate authentication (SSH-CA) public key. The point-of-sale device is further configured to store the host certificate, the user certificate, and the SSH-CA public key in the memory. The point-of-sale device is further configured to remove the one or more keys corresponding to the legacy communication channel from the memory.

[0009] According to an example, the point-of-sale device may further include an interface. The interface is configured to display a manual pairing reminder window after the host certificate, the user certificate, and the SSH-CA public key have been stored in the memory.

[0010] According to an example, the point-of-sale device is further configured to receive, via an interface of the point-of-sale device, a manual pair device command. The point-of-sale device is further configured to transmit, via the transceiver, a second start pairing command to the site controller upon receiving the manual pair device command. The point-of-sale device is further configured to receive, via the interface, a second one-time password. The point-of-sale device is further configured to generate, via the processor, a second host CSR and a second user CSR. The point-of-sale device is further configured to transmit, via the transceiver, the second host CSR and the second user CSR to the site controller. The point-of-sale device is further configured to receive, via the transceiver, a second host certificate corresponding to the second host CSR, a second user certificate corresponding to the second user CSR, and a second

SSH-CA public key. The point-of-sale device is further configured to store the host certificate, the user certificate, and the second SSH-CA public key in the memory.

[0011] According to an example, the point-of-sale device is further configured to disable the manual pairing reminder window after the second host certificate, the second user certificate, and the second SSH-CA public key have been stored in the memory.

[0012] According to an example, the second host CSR is based on the second one-time password. According to a further example, the second user CSR is based on the second one-time password.

[0013] Generally, in another aspect, a site controller is provided. The site controller includes a memory storing one or more keys corresponding to a legacy communications channel. The site controller further includes a processor and a transceiver.

[0014] The site controller is configured to receive, via the transceiver over the legacy communication channel, a start pairing command from a point-of-sale device. The site controller is further configured to generate, via the processor, a one-time password upon receiving the start pairing command. The site controller is further configured to transmit, via the transceiver over the legacy communication channel, the one-time password to the point-of-sale device. The site controller is further configured to receive, via the transceiver, a host CSR and a user CSR from the point-of-sale device. The host CSR may be based on the one-time password. The user CSR may be based on the one-time password. The site controller is further configured to generate, via the processor, a host certificate based on the host CSR. The site controller is further configured to generate, via the processor, a user certificate based on the user CSR. The site controller is further configured to transmit, via the transceiver, the host certificate, the user certificate, and an SSH-CA public key to the point-of-sale device.

[0015] According to an example, the site controller is further configured to receive, via the transceiver, a second start pairing command from a point-of-sale device. The second start pairing command corresponds to a user providing a manual pair device command to the point-of-sale device. The site controller is further configured to generate, via the processor, a second one-time password upon receiving the second start pairing command. The site controller is further configured to display the second one-time password. The site controller is further configured to receive, via the transceiver, a second host CSR and a second user CSR from the point-of-sale device. The site controller is further configured to generate, via the processor, a second host certificate based on the host CSR. The site controller is further configured to generate, via the processor, a second user certificate based on the user CSR. The site controller

is further configured to transmit, via the transceiver, the second host certificate, the second user certificate, and a second SSH-CA public key to the point-of-sale device.

[0016] According to an example, the second host CSR is based on the second one-time password. Further to this example, the second user CSR is based on the second one-time password.

[0017] Generally, in another aspect, a method for pairing a point-of-sale device to a site controller is provided. The method includes transmitting, from the point-of-sale device to the site controller, via a legacy communication channel, a start pairing command. The method further includes generating, via the site controller, a one-time password upon receiving the start pairing command. The method further includes transmitting, via the legacy communication channel, the one-time password from the site controller to the point-of-sale device. The method further includes transmitting, from the point-of-sale device to the site controller, a host CSR. The method further includes transmitting, from the site controller to the point-of-sale device, a host certificate, and an SSH-CA public key. The host certificate is based on the host CSR. The method further includes transmitting, from the point-of-sale device to the site controller, a user CSR. The method further includes transmitting, from the site controller to the point-of-sale device, a user certificate based on the user CSR. The method further includes storing, via a memory of the point-of-sale device, the host certificate, the user certificate, and the SSH-CA public key. The method further includes removing one or more keys corresponding to the legacy communication channel from the memory of the point-of-sale device.

[0018] According to an example, the host CSR and the user CSR are based on the one-time password.

[0019] According to an example, the method further includes displaying, via an interface of the point-of-sale device, a manual pairing reminder window after the host certificate, the user certificate, and the SSH-CA public key have been stored in the memory of the point-of-sale device.

[0020] According to an example, the method further includes receiving, via an interface of the point-of-sale device, a manual pair device command. The method further includes transmitting, from the point-of-sale device to the site controller, a second start pairing command upon receiving the manual pair device command. The method further includes generating, via the site controller, a second one-time password upon receiving the second start pairing command. The method further includes displaying, via the site controller, the second one-time password. The method further includes receiving, via the interface of the point-of-sale device, the second one-time password. The method further includes transmitting, from the

point-of-sale device to the site controller, a second host CSR. The method further includes transmitting, from the site controller to the point-of-sale device, a second host certificate and a second SSH-CA public key, wherein the second host certificate is based on the second host CSR. The method further includes transmitting, from the point-of-sale device to the site controller, a second user CSR. The method further includes transmitting, from the site controller to the point-of-sale device, a second user certificate based on the user CSR. The method further includes storing, via the memory of the point-of-sale device, the second host certificate, the second user certificate, and the second SSH-CA public key.

[0021] According to an example, the second host CSR and the second user CSR are based on the one-time password.

[0022] According to an example, the method further includes disabling the manual pairing reminder window after the second host certificate, the second user certificate, and the second SSH-CA public key have been stored in the memory of the point-of-sale device.

[0023] In various implementations, a processor or controller may be associated with one or more storage media (generically referred to herein as "memory," e.g., volatile and non-volatile computer memory such as RAM, PROM, EPROM, EEPROM, floppy disks, compact disks, optical disks, magnetic tape, etc.). In some implementations, the storage media may be encoded with one or more programs that, when executed on one or more processors and/or controllers, perform at least some of the functions discussed herein. Various storage media may be fixed within a processor or controller or may be transportable, such that the one or more programs stored thereon can be loaded into a processor or controller so as to implement various aspects as discussed herein. The terms "program" or "computer program" are used herein in a generic sense to refer to any type of computer code (e.g., software or microcode) that can be employed to program one or more processors or controllers.

[0024] It should be appreciated that all combinations of the foregoing concepts and additional concepts discussed in greater detail below (provided such concepts are not mutually inconsistent) are contemplated as being part of the inventive subject matter disclosed herein. In particular, all combinations of claimed subject matter appearing at the end of this disclosure are contemplated as being part of the inventive subject matter disclosed herein. It should also be appreciated that terminology explicitly employed herein that also may appear in any disclosure incorporated by reference should be accorded a meaning most consistent with the particular concepts disclosed herein.

[0025] These and other aspects of the various embodiments will be apparent from and elucidated with reference to the embodiment(s) described hereinafter.

Brief Description of the Drawings

[0026] In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the various embodiments.

[0027] FIG. 1 is a system diagram of a payment system, in accordance with an example.

[0028] FIG. 2 is a sequence diagram of a system-wide software upgrade process, in accordance with an example.

[0029] FIG. 3 is a sequence diagram of a manual pairing process, in accordance with an example.

[0030] FIG. 4 is a sequence diagram of an automatic pairing process, in accordance with an example.

[0031] FIG. 5 is a screenshot of a point-of-sale interface showing a manual pairing reminder pop-up window, in accordance with an example.

[0032] FIG. 6 is a screenshot of a point-of-sale interface showing a manual pairing reminder pop-up window, in accordance with a further example.

[0033] FIG. 7 is a screenshot of a controller client interface showing a One-Time Password pop-up window, in accordance with a further example.

[0034] FIG. 8 is a screenshot of a controller client interface showing a One-Time Password confirmation pop-up window, in accordance with a further example.

[0035] FIG. 9 is a screenshot of a controller client interface showing a One-Time Password code retrieval pop-up window, in accordance with a further example.

[0036] FIG. 10 is a screenshot of a point-of-sale interface showing a One-Time Password pairing code pop-up window, in accordance with a further example.

[0037] FIG. 11 is a screenshot of a point-of-sale interface showing a pairing confirmation screen, in accordance with a further example.

[0038] FIG. 12 is a schematic diagram of a point-of-sale device, in accordance with an example.

[0039] FIG. 13 is a schematic diagram of a site controller, in accordance with an example.

[0040] FIG. 14 is a flowchart of a method for pairing a point-of-sale device to a site controller, in accordance with an example.

[0041] FIG. 15 is a further flowchart of the method for pairing a point-of-sale device to a site controller, in accordance with an example.

Detailed Description of Embodiments

[0042] FIG. 1 illustrates a payment system 10. The payment system 10 includes three point-of-sale devices 100a, 100b, 100c, a site controller 200, a controller client 500, and a site router 600. The point-of-sale devices 100a-100c are operated by cashiers or other store employees to facilitate customer transactions. As shown in FIG. 12, the point-of-sale devices 100 may include a memory 125, an interface 165, a processor 175, and a transceiver 195. The interface 165 may include a display screen. In some examples, the point-of-sale devices 100a-100c may be configurable to operate in a self-checkout mode. In the self-checkout mode, the point-of-sale devices 100a-100c act as self-checkout terminals, and a customer may complete a transaction using the point-of-sale devices 100a-100c without assistance from an employee. The point-of-sale devices 100a-100c provide information regarding the transactions to a site controller 200. While FIG. 1 shows three point-of-sale devices 100a-100c, any practical number of point-of-sale devices 100 may be used according to the application of the user.

[0043] The site router 600 enables communication between the point-of-sale devices 100a, 100b, 100c, the site controller 200, and the controller client 500. The site router 600 may be communicatively coupled to the point-of-sale devices 100a, 100b, 100c, the site controller 200, and the controller client 500 via wired or wireless connection, such as Ethernet. In alternative examples, the site controller 200 may be directly connected to the point-of-sale devices 100a-100c via wired or wireless connection.

[0044] The site controller 200 receives, processes, and stores transaction information provided by the point-of-sale devices 100a-100c. As shown in FIG. 13, the site controller 200 may include a memory 225, a display 285, a processor 275, and a transceiver 295. Further, the site controller 200 transmits configuration information to the point-of-sale devices 100a-100c. This configuration information may determine various settings (regarding sales, payment, etc.) of each point-of-sale device 100a-100c. The site controller 200 may also transmit software upgrades to the point-of-sale devices 100a-100c. For example, when the site controller 200 undergoes a software upgrade, it may also transmit a corresponding upgrade to each point-of-sale device 100a-100c to ensure the upgrade of the site controller 200 is compatible with the point-of-sale devices 100a-100c.

[0045] The controller client 500 is communicatively coupled to the site controller 200, either directly or via site router 600, via wired or wireless connection. The controller client 500 can be used to configure the site controller 200, including facilitating pairing the site controller 200 to one or more of the point-of-sale devices 100a-100c. The controller client 500 may be

used to program additional settings of the site controller 200. In some examples, the controller client 500 may be a desktop computer, laptop computer, or a mobile device (such as a smartphone). In one example, the site controller 200 and the controller client 500 may be positioned locally relative to each other, such as in a backroom of a retail shop. In other examples, the site controller 200 may be located remotely relative to the controller client 500.

[0046] With further reference to FIG. 1, one of the point-of-sale devices 100a, 100b, 100c such as point-of-sale device 100a, may be paired to the site controller 200 via a manual pairing process. In this process, an authorized user initiates a pairing service controller client 500. In this example, the controller client 500 includes a browser connected to the site controller 200 to facilitate the pairing process. The authorized user may have to enter a password or other credentials to initiate the pairing process.

[0047] The user then must initiate the pairing process on the point-of-sale device 100a. This may be done by pressing a "pair device" button. The "pair device" button may be a hard key or soft key arranged on the point-of-sale device 100a. The "pair device" button may also be a virtual button displayed on the interface 165 (such as a graphical user interface) of the point-of-sale device 100a. Pressing the "pair device" button transmits a "start pairing" command 112 (see FIG. 12) to the site controller 200. Other methods of initiating the transmission of the start pairing command 112 for manual pairing may be used.

[0048] Upon receiving the start pairing command 112, the site controller 200 generates a one-time password 210 (see FIG. 13) unique to this manual pairing session. The authorized user may read the one-time password 210 either (1) from the browser of the controller client 500 or (2) from a two-digit, seven-segment display 285 (such as a two-digit, seven-segment display) on the site controller 200. The authorized user then returns to the point-of-sale device 100a and enters the one-time password 210 via interface 165. Entering the one-time password 210 triggers the point-of-sale device 100a to transmit two signing requests to the site controller 200; one signing request for the point-of-sale device 100a itself (the "host" request 114 (see FIG. 12)), and one signing request for the specific user logging into the point-of-sale device 100a (the "user" request 116 (see FIG. 12). In some examples, this user may be different from the authorized user who initiated the pairing processes via the controller client 500.

[0049] In an alternate example, the one-time password 210 may be read off the display 285 of the site controller 200 by a camera attached to the point-of-sale device 100a, thus ensuring physical proximity between the site controller 200 and the point-of-sale device 100a. In a further example, the one-time password 210 could be transmitted through the air, rather than displayed, by means such as vibrations or magnetic impulses, to the point-of-sale device 100a.

[0050] Upon receiving the signing requests, the site controller 200 generates a signed host certificate 212 (see FIG. 13) and a signed user certificate 214 (see FIG. 13), and transmits the certificates 212, 214 to the point-of-sale device 100a. The point-of-sale device 100a receives the certificates 212, 214, reboots, and is then able to securely communicate with the site controller 200.

[0051] With continued reference to FIG. 1, an auto-pairing process may also be performed to enable communication between the point-of-sale device 100a and the site controller 200. In a typical example, and as described above, the auto-pairing process is performed as part of an overall software upgrade applied to the point-of-sale device 100a and the site controller 200. In this way, the point-of-sale device 100a and the site controller 200 may communicate initially without performing the more onerous manual pairing. This allows for a retail shop to process payments and transactions immediately following the software upgrade, even if the employees lack the technical skills or credentials to perform the manual pairing process. For increased security, the point-of-sale device 100a will provide recurring reminders to perform a manual pairing process at some point in the near future.

[0052] The auto-pairing process begins with the internal application programming interface (API) of the client controller 500 activating the pairing service as part of the software upgrade of the site controller 200. Similarly, the software upgrade uses the API of the point-of-sale device 100a to initiate the pairing process. As with the manual pairing process, the point-of-sale device 100a transmits a “start pairing” command 102 (see FIG. 12) to the site controller 200. This triggers the site controller 200 to generate a one-time password 202 (see FIG. 13) unique to this pairing session.

[0053] The auto-upgrade process then transmits the one-time password 202 to the point-of-sale device 100a via an existing legacy communications channel 50 (see FIG. 4). Depending on the system architecture and configuration, the one-time password 210 may be transmitted by either the site controller 200 or the controller client 500. The point-of-sale device 100a receives the one-time password 202, and enters the one-time password 202 via API call. Entering the one-time password 202 triggers the point-of-sale device 100a to transmit host and user signing requests 104, 106 (see FIG. 12) to the site controller 200. The site controller 200 receives the requests and generates signed host and user certificates 204, 206 (see FIG. 13) to the point-of-sale device 100a. The point-of-sale device 100a then ends the pairing process, completes the upgrade software process, and reboots into normal point-of-sale operation.

[0054] Thus, the auto-upgrade removes human intervention from the pairing process by automatically (1) activating the pairing service, (2) initiating the pairing of the point-of-sale

device 100a and the site controller 200, (3) transmitting the one-time password 202 to the point-of-sale device 100a via the existing legacy communication channel 50, and (4) automatically entering the one-time password 202 into the point-of-sale device 100a. While this auto-upgrade process is significantly easier for users to implement, and is more secure than distributing sensitive assets (like private keys) with the software upgrade bundle, it is less secure than requiring on-site employees to manually read a one-time password 210 from the site controller 200 or the controller client 500, and then manually enter the one-time password 210 into the point-of-sale device 100a. Therefore, for increased security, reminders 108 (see FIG. 12) will be provided to the user of the auto-paired point-of-sale device 100a to perform manual pairing.

[0055] FIG. 2 illustrates the timing of the auto-pairing process in relation to the various steps of the software upgrade process. As shown, the first phase on the software upgrade includes a site controller hard drive 200a receiving and authenticating the upgrade. The site controller 200 is then notified of the received software upgrade. The site controller 200 then performs an evaluation, checks prerequisites for the software upgrade, and backs up configurations and payment/transaction totals. The software is then installed on both the site controller 200 as well as the connected point-of-sale devices 100. The site controller 200 then restores any data required to make the site functional. The site controller 200 and point-of-sale devices 100 are initialized, and the auto-pairing of the site controller 200 and the point-of-sale devices 100 occurs. Conducting the auto-pairing makes the overall site functional to conduct sales. Following the auto-pairing, historical data is restored to the site controller 200, and clean-up activities complete the software upgrade process.

[0056] FIG. 3 shows a sequence diagram of the aforementioned manual pairing process. The manual pairing process utilizes the secure shell (SSH) protocol, specifically secure shell certificate authentication (SSH-CA). While FIG. 3 depicts the manual pairing of a single point-of-sale device 100 to a site controller 200, any number of point-of-sale devices 100 may be paired to the site controller 200 (or some other device) via manual pairing. Further, other types of devices (such as audio-visual gear) may be paired to the site controller 200 according to the depicted manual pairing process.

[0057] As shown in the non-limiting example of FIG. 3, the manual pairing process is initiated by site personnel manually entering a manual pair device command 110 (see FIG. 12) into the interface 165 (see FIG. 12) of point-of-sale device 100. The “start pairing” command 112 (see FIG. 12) is passed to the site controller 200. The site controller 200 generates and displays a one-time password 210 via display 285. The one-time password 210 may be displayed on either the site controller 200 itself, and/or on a browser of a controller client 500

for the site-personnel to read. The site controller 200 also generates a nonce to be used for the presently occurring pairing session. The session nonce is then passed to the point-of-sale device 100. The site controller 200 stores the one-time password 210 and nonce from this manual pairing process in memory 225 (see FIG. 13) to use in subsequent processing steps.

[0058] The point-of-sale device 100 prompts the site-personnel to enter the one-time password 210. Once the one-time password 210 is received, the point-of-sale device 100 issues at least two certificate signing requests (CSRs) to the site controller 200. First, the point-of-sale device 100 issues a CSR related to the specific point-of-sale device 100 being paired, referred to as a host CSR 114 (see FIG. 12). The host CSR 114 includes a host hash-based message authentication code (HMAC) and hostinfo. The point-of-sale device 100 generates the message HMAC based on the session nonce, the one-time password 210, and the hostID. Upon receiving the host CSR 114, the site controller 200 generates a host certificate 212 (see FIG. 13), and transmits the certificate 212 and a secure shell certificate authentication (SSH-CA) public key 216 (see FIG. 13) to the point-of-sale device 100. The point-of-sale device 100 then validates the received message using the message HMAC.

[0059] Second, the point-of-sale device 100 also issues a CSR related to the individual user logged-in to the point-of-sale device 100, referred to as a user CSR 116 (see FIG. 12). The user CSR 116 includes a message HMAC and userinfo. The point-of-sale device 100 generates the message HMAC based on the session nonce, the one-time password 210, and the userID. The message HMAC may be based on additional information where relevant. Upon receiving the user CSR 106, the site controller 200 generates a user certificate 214 (see FIG. 13), and transmits the certificate 214 to the point-of-sale device 100. The point-of-sale device 100 then validates the received message using the message HMAC. Additional user CSRs 116 may be issued for other individuals using the point-of-sale device 100.

[0060] The validation of the messages is based on standard HMAC architecture. Notably, the nonce (or the "seed" of the HMAC) is shared between the site controller 200 and the point-of-sale device 100 over their wired or wireless connection. However, the one-time password 210 (or the "passphrase" of the HMAC) is conveyed by a person reading the password 210 off the site controller 200. The nonce and the passphrase combine to form the "key" of the HMAC algorithm. Thus, validation of the received certificates requires both the point-of-sale device 100 and the site controller 200 to know the same nonce and one-time password 210. In some examples, the nonce is at least 128 bits, while the one-time password 210 is at least six hexadecimal digits.

[0061] Having received the certificates 212, 214 and the SSH-CA public key 216, the point-of-sale device 100 has all of the information needed to facilitate communication with the site controller 200. Accordingly, the point-of-sale device 10 transmits an "end pairing" command to the site controller 200, which triggers the site controller 200 to stop displaying the one-time password 210. The point-of-sale device 100 stores the received certificates 212, 214 and the SSH-CA public key 216 in memory 125 (see FIG. 12), and issues a notification to the site personnel that the manual pairing process has completed.

[0062] FIG. 4 shows a sequence diagram of the aforementioned automatic pairing process. As with the manual pairing process, the automatic pairing process utilizes the SSH-CA protocol. As previously mentioned, the automatic pairing process occurs during the software upgrade, typically after the installation of the upgraded software, but before the historic data has been restored to the site controller 200 and the point-of-sale devices 100. The automatic pairing process leverages existing legacy communication channels 50 between the point-of-sale device 10 and the site controller 200 to automate the manually performed aspects of manual pairing. The legacy communication channels 50 may utilize any practical protocol. In one example, the legacy communication channel 50 is an SSH channel based on public-private key pairs provided with a previously installed software bundle. The automatic pairing process is more secure than the legacy communication channel 50, as the automatic pairing process generates certificates 204, 206 (see FIG. 13) based on a one-time password 202 (see FIG. 13). In FIG. 4, the legacy communication channel 50 is indicated by bolded line.

[0063] While FIG. 4 depicts the automatic pairing of a single point-of-sale device 100 to a site controller 200, any number of point-of-sale devices 100 may be paired to the site controller 200 (or some other device) via automatic pairing. Further, other types of devices (such as audio-visual gear) may be paired to the site controller 200 according to the depicted manual pairing process as long as a legacy communication channel 50 exists between the device and the site controller 200.

[0064] As shown in the non-limiting example of FIG. 4, the point-of-sale device 100 initiates the automatic pairing process by transmitting a start auto-pairing command to the site controller 200 via the legacy communication channel 50. The site controller 200 then starts the pairing service.

[0065] The point-of-sale device 100 then generates a "start pairing" command 102 (see FIG. 12), and transmits the command to the site controller 200. The site controller 200 generates and displays a one-time password 202 (see FIG. 13) in response to receiving the "start pairing" command 102. Rather than relying on site-personnel to read the one-time password 202 off of

the seven-segment display 285 (see FIG. 13) of the site controller 200 or the controller client 500 (see FIG. 1), the site controller 200 transmits the one-time password 200 to the point-of-sale device 100 via the legacy communications channel 50. Accordingly, in some examples of the automatic pairing process, the site controller 200 does not display the one-time password 202. The point-of-sale device 100 also receives a nonce generated by the site controller 200. The site controller 200 stores the one-time password 202 and nonce to use in subsequent processing steps.

[0066] Having received the one-time password 202 and the nonce, the point-of-sale device 100 issues at least two CSRs to the site controller 200. First, the point-of-sale device 100 issues a host CSR 104 (see FIG. 12). The host CSR 104 includes a message HMAC and hostinfo. The point-of-sale device 100 generates the message HMAC based on the session nonce, the one-time password 202, and the hostID. Upon receiving the host CSR 104, the site controller 200 generates a host certificate 204 (see FIG. 13), and transmits the certificate 204 and an SSH-CA public key 208 (see FIG. 13) to the point-of-sale device 100. The point-of-sale device 100 then validates the received message using the message HMAC.

[0067] Second, the point-of-sale device 100 also issues a user CSR 106 (see FIG. 12). The user CSR 106 includes a message HMAC and userinfo. The point-of-sale device 100 generates the message HMAC based on the session nonce, the one-time password 202, and the userID. The message HMAC may be based on additional information where relevant. Upon receiving the user CSR 106, the site controller 200 generates a user certificate 206, and transmits the certificate to the point-of-sale device 100. The point-of-sale device 100 then validates the received message using the message HMAC.

[0068] Having received the certificates 204, 206 and the SSH-CA public key 208, the point-of-sale device 100 transmits an “end pairing” command to the site controller 200, which triggers the site controller 200 to stop displaying the one-time password 202 (if the one-time password 202 was displayed earlier in the sequence). The point-of-sale device 100 stores the received certificates 204, 206 and the SSH-CA public key 208 in memory 125 (see FIG. 12), and issues a notification to the site personnel that the manual pairing process has completed. The point-of-sale device 100 then notifies the site controller 200 that auto-pairing has completed, resulting in the site controller 200 ending pairing service. Importantly, the point-of-sale device 100 also removes any keys related to the legacy communications channel 50, thereby requiring the point-of-sale device 100 to communicate with the site controller 200 via the more secure auto-paired channel. Following successful auto-pairing, the interface 165 of

the point-of-sale device 100 will display reminder messages to encourage the site personnel to manually pair the point-of-sale device 100 to the site controller 200.

[0069] FIG. 5 shows an example screenshot of an interface 165 of a point-of-sale device 100 (see FIG. 1) in use after the software upgrade has been installed. As previously stated, the "auto-pairing" immediately following the software installation allows the point-of-sale device 100 to remain in communication with the site controller 200 (see FIG. 1). As such, a cashier may use the point-of-sale device 100 to process customer transactions before manual pairing is performed. However, as manual pairing provides a greater degree of security than "auto-pairing," the cashier will be reminded to perform manual pairing through a recurring manual pairing required pop-up window 108. As shown in FIG. 5, the manual pairing required pop-up window 108 overlays the point-of-sale interface 165, requiring the cashier to acknowledge the pop-up window 108 by clicking "OK" to continue using the point-of-sale device 100. This pop-up window 108 may be configured to appear periodically, such as every 5 minutes. Alternatively, the pop-up window 108 may be configured to appear in response to certain actions performed with the point-of-sale device 100 (such as after a completed transaction) until a trusted relationship is established by manually pairing the point-of-sale device 100 and the site controller 200. The point-of-sale device 100 may determine the status of the trusted relationship by evaluating a variable, flag, or token provided or set when the trusted relationship is formed. This manual pairing reminder window 108 is meant to remind the cashier to either perform manual pairing themselves, or find a skilled and credentialed employee to perform the pairing. Once the manual pairing is performed, the interface 165 will no longer show the manual pairing reminder pop-up window 108.

[0070] FIG. 6 shows a variation of FIG. 5, wherein the manual pairing reminder pop-up window 108 is displayed when the point-of-sale device 100 is in self-checkout mode. In self-checkout mode, the point-of-sale device 100 functions as a self-checkout terminal, allowing customers to complete their purchase unaided by a cashier. Displaying the manual pairing reminder pop-up window 108 may cause a customer to call for help, leading an employee to perform manual pairing.

[0071] FIG. 7 shows a configuration screen 565 of a controller client 500 (see FIG. 1) communicatively coupled to a site controller 200 (see FIG. 1). When an employee decides to manually pair a point-of-sale device 100 (see FIG. 1) with the site controller 200, they are required to enter a new one-time password 210 (see FIG. 12) into the point-of-sale device 100. This new one-time password 210 is generated by the site controller 200. In one example, for security purposes, the one-time password 210 may be found by viewing a status display 285

(such as a two-digit, seven segment display) (see FIG. 13) physically located on the site controller 200. The display of the one-time password 210 may be triggered by a user clicking the "Generate OTP" wording shown on a pop-up window in the configuration screen 565. FIG. 8 shows a pop-up message instructing a user to view the status display 285 of the site controller 200 to retrieve the one-time password 210. By restricting access to the one-time password 210 to individuals within physical proximity of the site controller 200, the threat of remote cyber-attacks is eliminated. Further, this one-time password 210 may also be required to be entered into the controller client 500 to allow an employee to initiate the pairing service of the site controller 200.

[0072] Once the one-time password 210 has been entered, the user initiates the pairing service on both the site controller 200 and the point-of-sale device 100. As shown in FIG. 9, the user can retrieve the one-time password from the interface 565 of the controller client 500. In this case, the one-time password is 208134. While the one-time password 210 of this example includes six hexadecimal digits, additional digits may be included to increase security. As shown in FIG. 10, the user may then enter the one-time password 210 into a pairing code entry pop-up window of the interface 165 of the point-of-sale device 100. As the same one-time password 210 was generated by the site controller 200, the manual pairing process has been completed, and a secure, trusted relationship now exists between the point-of-sale device 100 and the site controller 200. The formation of the trusted relationship results in the display of the successful pairing screen on the interface 165 of the point-of-sale device 100 as shown in FIG. 11. Accordingly, the point-of-sale device 100 will no longer display the manual pairing reminder pop-up window 108 shown in FIGS. 5 and 6.

[0073] FIG. 12 is a schematic illustration of a point-of-sale device 100. Generally, the point-of-sale device 100 includes a memory 125, an interface 165, a processor 175, and a transceiver 195. The memory 125 stores a wide array of data received and/or generated by the point-of-sale device 100 as part of the auto-pairing and manual pairing processes. Prior to the pairing processes, the memory 125 stores one or more legacy keys 52 corresponding to a legacy communications channel 50 (see FIG. 4). As part of the auto-pairing process, the memory 125 stores data received via the transceiver 195, including a one-time password 202, a host certificate 204, a user certificate 206, and an SSH-CA public key 208. The memory 125 also stores data generated by the processor 175 to be transmitted via the transceiver 195, including a start pairing command 102, a host CSR 104, and a user CSR 106. As part of the manual pairing process completed after auto-pairing, the memory 125 stores data received via the transceiver 195, including a manual pairing ("MP") one-time password 210, an MP host

certificate 212, an MP user certificate 214, and an MP SSH-CA public key 216. The memory 125 also stores data generated by the processor 175 to be transmitted via the transceiver 195, including an MP start pairing command 112, an MP host CSR 114, and an MP user CSR 116. The memory 125 also stores a manual pair device command 110 received via the interface 165 to trigger the manual pairing process. Following auto-pairing, the interface 165 also displays a manual pairing reminder pop-up window 108 until manual pairing has been completed.

[0074] FIG. 13 is a schematic illustration of a site controller 200. Generally, the point-of-sale device 100 includes a memory 225, a processor 275, a display 285, and a transceiver 295. The memory 225 stores a wide array of data received and/or generated by the site controller 200 as part of the auto-pairing and manual pairing processes. Prior to the pairing processes, the memory 225 stores one or more legacy keys 52 corresponding to a legacy communications channel 50 (see FIG. 4). As part of the auto-pairing process, the memory 225 stores data received via the transceiver 295, including a start pairing command 102, a host CSR 104, and a user CSR 106. The memory 225 also stores data generated by the processor 275 to be transmitted via the transceiver 295, including a one-time password 202, a host certificate 204, a user certificate 206, and an SSH-CA public key 208. As part of the manual pairing process completed after auto-pairing, the memory 225 stores data received via the transceiver 195, including a manual pair device command 110, a manual pairing ("MP") start pairing command 112, an MP host CSR 114, and an MP user CSR 116. The memory 225 also stores data generated by the processor 275 to be transmitted via the transceiver 195, including an MP one-time password 210, an MP host certificate 212, an MP user certificate 214, and an MP SSH-CA public key 216. The display 285 may be a seven-segment display showing the one-time password 202 of the MP one-time password 210 generated by the processor 275.

[0075] FIGS. 14 and 15 show a flowchart of a method 900 for pairing a point-of-sale device to a site controller. The method 900 includes transmitting 902, from the point-of-sale device to the site controller, via a legacy communication channel, a start pairing command. The method 900 further includes generating 904, via the site controller, a one-time password upon receiving the start pairing command. The method 900 further includes transmitting 906, via the legacy communication channel, the one-time password from the site controller to the point-of-sale device. The method 900 further includes transmitting 908, from the point-of-sale device to the site controller, a host CSR. The method 900 further includes transmitting 910, from the site controller to the point-of-sale device, a host certificate, and an SSH-CA public key. The host certificate is based on the host CSR. The method 900 further includes transmitting 912, from the point-of-sale device to the site controller, a user CSR. The method 900 further includes

transmitting 914, from the site controller to the point-of-sale device, a user certificate based on the user CSR. The method 900 further includes storing 916, via a memory of the point-of-sale device, the host certificate, the user certificate, and the SSH-CA public key. The method 900 further includes removing 918 one or more keys corresponding to the legacy communication channel from the memory of the point-of-sale device. According to an example, the host CSR and the user CSR are based on the one-time password.

[0076] According to an example, the method 900 further includes displaying 920, via an interface of the point-of-sale device, a manual pairing reminder window after the host certificate, the user certificate, and the SSH-CA public key have been stored in the memory of the point-of-sale device.

[0077] According to an example, the method 900 further includes receiving 922, via an interface of the point-of-sale device, a manual pair device command. The method 900 further includes transmitting 924, from the point-of-sale device to the site controller, a second start pairing command upon receiving the manual pair device command. The method 900 further includes generating 926, via the site controller, a second one-time password upon receiving the second start pairing command. The method 900 further includes displaying 928, via the site controller, the second one-time password. The method 900 further includes receiving 930, via the interface of the point-of-sale device, the second one-time password. The method 900 further includes transmitting 932, from the point-of-sale device to the site controller, a second host CSR. The method 900 further includes transmitting 934, from the site controller to the point-of-sale device, a second host certificate and a second SSH-CA public key, wherein the second host certificate is based on the second host CSR. The method 900 further includes transmitting 936, from the point-of-sale device to the site controller, a second user CSR. The method 900 further includes transmitting 938, from the site controller to the point-of-sale device, a second user certificate based on the user CSR. The method 900 further includes storing 940, via the memory of the point-of-sale device, the second host certificate, the second user certificate, and the second SSH-CA public key. According to an example, the second host CSR and the second user CSR are based on the one-time password.

[0078] According to an example, the method 900 further includes disabling 942 the manual pairing reminder window after the second host certificate, the second user certificate, and the second SSH-CA public key have been stored in the memory of the point-of-sale device.

[0079] All definitions, as defined and used herein, should be understood to control over dictionary definitions, definitions in documents incorporated by reference, and/or ordinary meanings of the defined terms.

[0080] The indefinite articles "a" and "an," as used herein in the specification and in the claims, unless clearly indicated to the contrary, should be understood to mean "at least one."

[0081] The phrase "and/or," as used herein in the specification and in the claims, should be understood to mean "either or both" of the elements so conjoined, i.e., elements that are conjunctively present in some cases and disjunctively present in other cases. Multiple elements listed with "and/or" should be construed in the same fashion, i.e., "one or more" of the elements so conjoined. Other elements may optionally be present other than the elements specifically identified by the "and/or" clause, whether related or unrelated to those elements specifically identified.

[0082] As used herein in the specification and in the claims, "or" should be understood to have the same meaning as "and/or" as defined above. For example, when separating items in a list, "or" or "and/or" shall be interpreted as being inclusive, i.e., the inclusion of at least one, but also including more than one, of a number or list of elements, and, optionally, additional unlisted items. Only terms clearly indicated to the contrary, such as "only one of" or "exactly one of," or, when used in the claims, "consisting of," will refer to the inclusion of exactly one element of a number or list of elements. In general, the term "or" as used herein shall only be interpreted as indicating exclusive alternatives (i.e. "one or the other but not both") when preceded by terms of exclusivity, such as "either," "one of," "only one of," or "exactly one of."

[0083] As used herein in the specification and in the claims, the phrase "at least one," in reference to a list of one or more elements, should be understood to mean at least one element selected from any one or more of the elements in the list of elements, but not necessarily including at least one of each and every element specifically listed within the list of elements and not excluding any combinations of elements in the list of elements. This definition also allows that elements may optionally be present other than the elements specifically identified within the list of elements to which the phrase "at least one" refers, whether related or unrelated to those elements specifically identified.

[0084] It should also be understood that, unless clearly indicated to the contrary, in any methods claimed herein that include more than one step or act, the order of the steps or acts of the method is not necessarily limited to the order in which the steps or acts of the method are recited.

[0085] In the claims, as well as in the specification above, all transitional phrases such as "comprising," "including," "carrying," "having," "containing," "involving," "holding," "composed of," and the like are to be understood to be open-ended, i.e., to mean including but

not limited to. Only the transitional phrases "consisting of" and "consisting essentially of" shall be closed or semi-closed transitional phrases, respectively.

[0086] The above-described examples of the described subject matter can be implemented in any of numerous ways. For example, some aspects may be implemented using hardware, software or a combination thereof. When any aspect is implemented at least in part in software, the software code can be executed on any suitable processor or collection of processors, whether provided in a single device or computer or distributed among multiple devices/computers.

[0087] The present disclosure may be implemented as a system, a method, and/or a computer program product at any possible technical detail level of integration. The computer program product may include a computer readable storage medium (or media) having computer readable program instructions thereon for causing a processor to carry out aspects of the present disclosure.

[0088] The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

[0089] Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers,

firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

[0090] Computer readable program instructions for carrying out operations of the present disclosure may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, configuration data for integrated circuitry, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Smalltalk, C++, or the like, and procedural programming languages, such as the "C" programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some examples, electronic circuitry including, for example, programmable logic circuitry, field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present disclosure.

[0091] Aspects of the present disclosure are described herein with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products according to examples of the disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer readable program instructions.

[0092] The computer readable program instructions may be provided to a processor of a, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. These computer readable

program instructions may also be stored in a computer readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a particular manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the function/act specified in the flowchart and/or block diagram or blocks.

[0093] The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0094] The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various examples of the present disclosure. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of instructions, which comprises one or more executable instructions for implementing the specified logical function(s). In some alternative implementations, the functions noted in the blocks may occur out of the order noted in the Figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts or carry out combinations of special purpose hardware and computer instructions.

[0095] Other implementations are within the scope of the following claims and other claims to which the applicant may be entitled.

[0096] While various examples have been described and illustrated herein, those of ordinary skill in the art will readily envision a variety of other means and/or structures for performing the function and/or obtaining the results and/or one or more of the advantages described herein, and each of such variations and/or modifications is deemed to be within the scope of the examples described herein. More generally, those skilled in the art will readily appreciate that all parameters, dimensions, materials, and configurations described herein are meant to be exemplary and that the actual parameters, dimensions, materials, and/or configurations will depend upon the specific application or applications for which the teachings is/are used. Those

skilled in the art will recognize, or be able to ascertain using no more than routine experimentation, many equivalents to the specific examples described herein. It is, therefore, to be understood that the foregoing examples are presented by way of example only and that, within the scope of the appended claims and equivalents thereto, examples may be practiced otherwise than as specifically described and claimed. Examples of the present disclosure are directed to each individual feature, system, article, material, kit, and/or method described herein. In addition, any combination of two or more such features, systems, articles, materials, kits, and/or methods, if such features, systems, articles, materials, kits, and/or methods are not mutually inconsistent, is included within the scope of the present disclosure.

Claims

What is claimed is:

1. A point-of-sale device comprising a memory storing one or more keys corresponding to a legacy communications channel, a processor, and a transceiver, the point-of-sale device configured to:

transmit, via the transceiver over the legacy communication channel, a start pairing command to a site controller;

receive, via the transceiver over the legacy communication channel, a one-time password generated by the site controller;

generate, via the processor, a host certificate signing request (CSR) and a user CSR;

transmit, via the transceiver, the host CSR and the user CSR to the site controller;

receive, via the transceiver, a host certificate corresponding to the host CSR, a user certificate corresponding to the user CSR, and a secure shell certificate authentication (SSH-CA) public key;

store the host certificate, the user certificate, and the SSH-CA public key in the memory; and

remove the one or more keys corresponding to the legacy communication channel from the memory.

2. The point-of-sale device of claim 1, wherein the host CSR is based on the one-time password.

3. The point-of-sale device of claim 1, wherein the user CSR is based on the one-time password.

4. The point-of-sale device of claim 1 further comprising an interface configured to display a manual pairing reminder window after the host certificate, the user certificate, and the SSH-CA public key have been stored in the memory.

5. The point-of-sale device of claim 4, wherein the point-of-sale device is further configured to:

receive, via the interface, a manual pair device command;

transmit, via the transceiver, a second start pairing command to the site controller upon receiving the manual pair device command;

receive, via the interface, a second one-time password;

generate, via the processor, a second host CSR and a second user CSR;

transmit, via the transceiver, the second host CSR and the second user CSR to the site controller;

receive, via the transceiver, a second host certificate corresponding to the second host CSR, a second user certificate corresponding to the second user CSR, and a second SSH-CA public key; and

store the host certificate, the user certificate, and the second SSH-CA public key in the memory.

6. The point-of-sale device of claim 5, wherein the point-of-sale device is further configured to disable the manual pairing reminder window after the second host certificate, the second user certificate, and the second SSH-CA public key have been stored in the memory.

7. The point-of-sale device of claim 5, wherein the second host CSR is based on the second one-time password.

8. The point-of-sale device of claim 5, wherein the second user CSR is based on the second one-time password.

9. A site controller comprising a memory storing one or more keys corresponding to a legacy communications channel, a processor, and a transceiver, wherein the site controller is configured to:

receive, via the transceiver over the legacy communication channel, a start pairing command from a point-of-sale device;

generate, via the processor, a one-time password upon receiving the start pairing command;

transmit, via the transceiver over the legacy communication channel, the one-time password to the point-of-sale device;

receive, via the transceiver, a host certificate signing request (CSR) and a user CSR from the point-of-sale device;

generate, via the processor, a host certificate based on the host CSR;

generate, via the processor, a user certificate based on the user CSR; and

transmit, via the transceiver, the host certificate, the user certificate, and a secure shell certificate authentication (SSH-CA) public key to the point-of-sale device.

10. The site controller of claim 9, wherein the host CSR is based on the one-time password.

11. The site controller of claim 9, wherein the user CSR is based on the one-time password.

12. The site controller of claim 9, wherein the site controller is further configured to:

receive, via the transceiver, a second start pairing command from the point-of-sale device, wherein the second start pairing command corresponds to a user providing a manual pair device command to the point-of-sale device;

generate, via the processor, a second one-time password upon receiving the second start pairing command;

display the second one-time password;

receive, via the transceiver, a second host CSR and a second user CSR from the point-of-sale device;

generate, via the processor, a second host certificate based on the host CSR;

generate, via the processor, a second user certificate based on the user CSR; and

transmit, via the transceiver, the second host certificate, the second user certificate, and a second SSH-CA public key to the point-of-sale device.

13. The site controller of claim 12, wherein the second host CSR is based on the second one-time password.

14. The site controller of claim 12, wherein the second user CSR is based on the second one-time password.

15. A method for pairing a point-of-sale device to a site controller, comprising:

transmitting, from the point-of-sale device to the site controller, via a legacy communication channel, a start pairing command;

generating, via the site controller, a one-time password upon receiving the start pairing command;

transmitting, via the legacy communication channel, the one-time password from the site controller to the point-of-sale device;

transmitting, from the point-of-sale device to the site controller, a host certificate signing request (CSR);

transmitting, from the site controller to the point-of-sale device, a host certificate and a secure shell certificate authentication (SSH-CA) public key, wherein the host certificate is based on the host CSR;

transmitting, from the point-of-sale device to the site controller, a user CSR;

transmitting, from the site controller to the point-of-sale device, a user certificate based on the user CSR;

storing, via a memory of the point-of-sale device, the host certificate, the user certificate, and the SSH-CA public key; and

removing one or more keys corresponding to the legacy communication channel from the memory of the point-of-sale device.

16. The method of claim 15, wherein the host CSR and the user CSR are based on the one-time password.

17. The method of claim 15, further comprising displaying, via an interface of the point-of-sale device, a manual pairing reminder window after the host certificate, the user certificate, and the SSH-CA public key have been stored in the memory of the point-of-sale device.

18. The method of claim 17, further comprising:

receiving, via the interface, a manual pair device command;

transmitting, from the point-of-sale device to the site controller, a second start pairing command upon receiving the manual pair device command;

generating, via the site controller, a second one-time password upon receiving the second start pairing command;

displaying, via the site controller, the second one-time password;

receiving, via the interface of the point-of-sale device, the second one-time password;

transmitting, from the point-of-sale device to the site controller, a second host CSR;

transmitting, from the site controller to the point-of-sale device, a second host certificate and a second SSH-CA public key, wherein the second host certificate is based on the second host CSR;

transmitting, from the point-of-sale device to the site controller, a second user CSR;

transmitting, from the site controller to the point-of-sale device, a second user certificate based on the user CSR; and

storing, via the memory of the point-of-sale device, the second host certificate, the second user certificate, and the second SSH-CA public key.

19. The method of claim 18, wherein the second host CSR and the second user CSR are based on the one-time password.

20. The method of claim 18, further comprising disabling the manual pairing reminder window after the second host certificate, the second user certificate, and the second SSH-CA public key have been stored in the memory of the point-of-sale device.

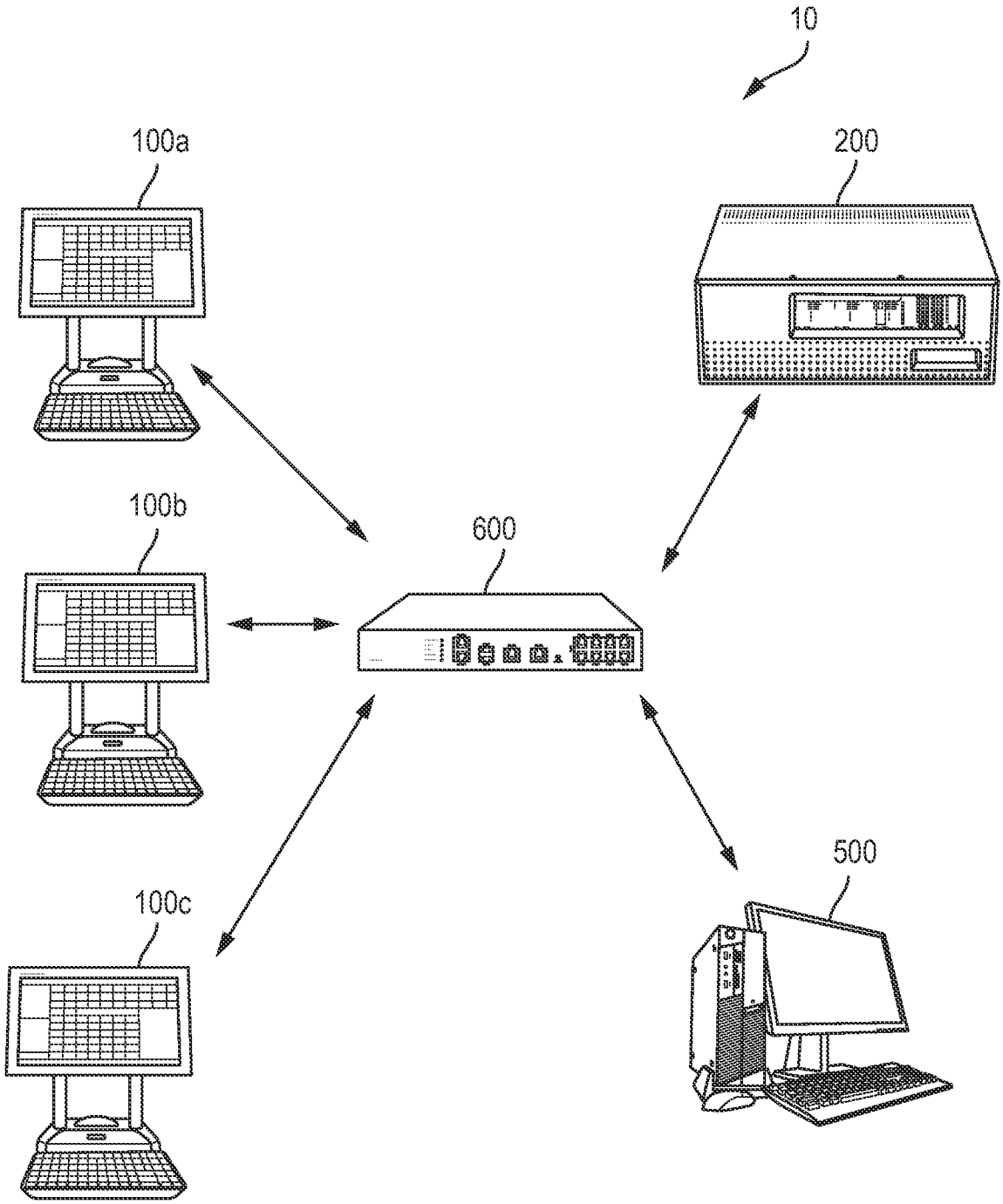


Fig. 1

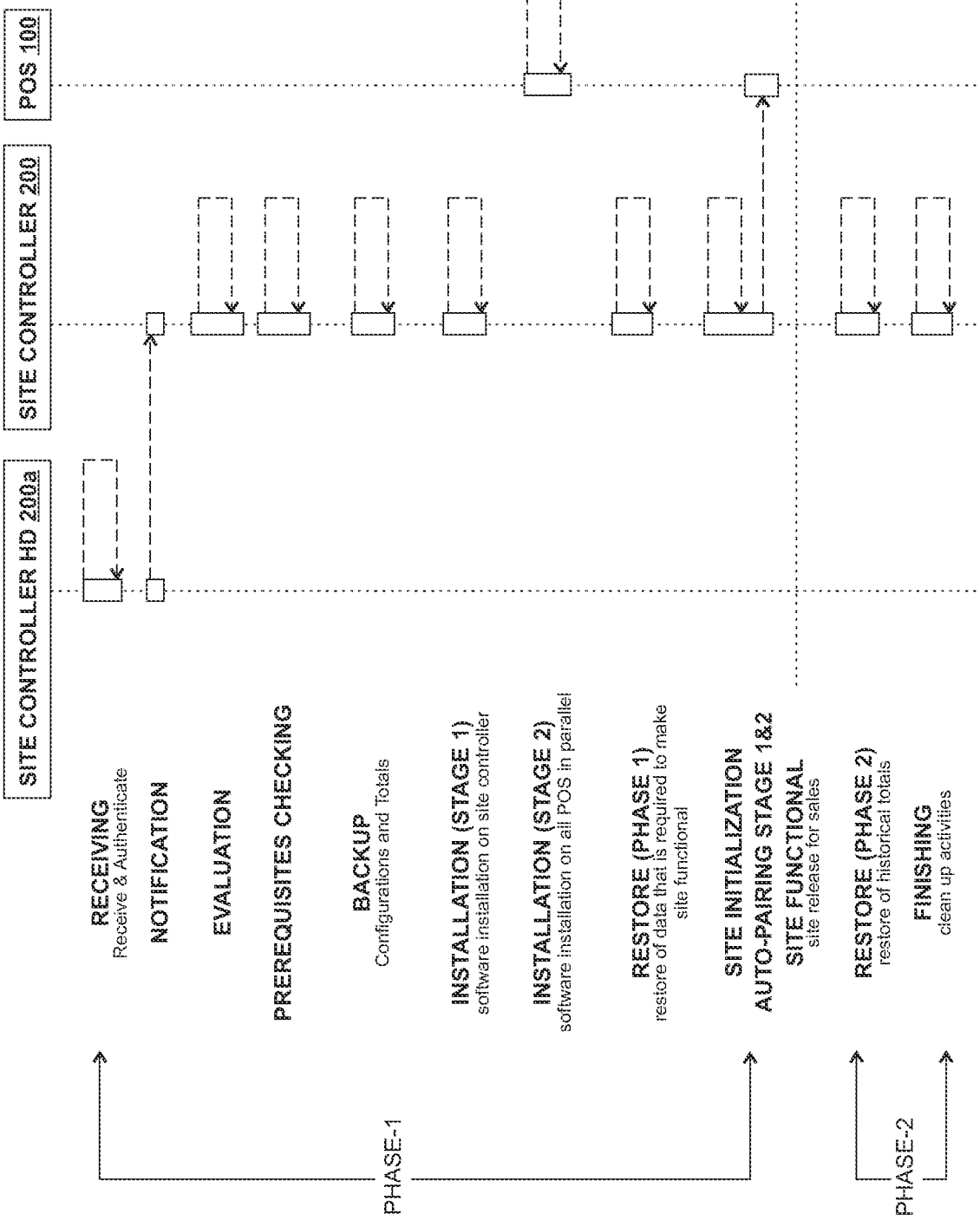

SITE CONTROLLER HD 200a
SITE CONTROLLER 200
POS 100
RECEIVING
Receive & Authenticate
NOTIFICATION
EVALUATION
PREREQUISITES CHECKING
BACKUP
Configurations and Totals
INSTALLATION (STAGE 1)
software installation on site controller
INSTALLATION (STAGE 2)
software installation on all POS in parallel
RESTORE (PHASE 1)
restore of data that is required to make site functional
SITE INITIALIZATION
AUTO-PAIRING STAGE 1&2
SITE FUNCTIONAL
site release for sales
RESTORE (PHASE 2)
restore of historical totals
FINISHING
clean up activities
PHASE-1
PHASE-2

Fig. 2

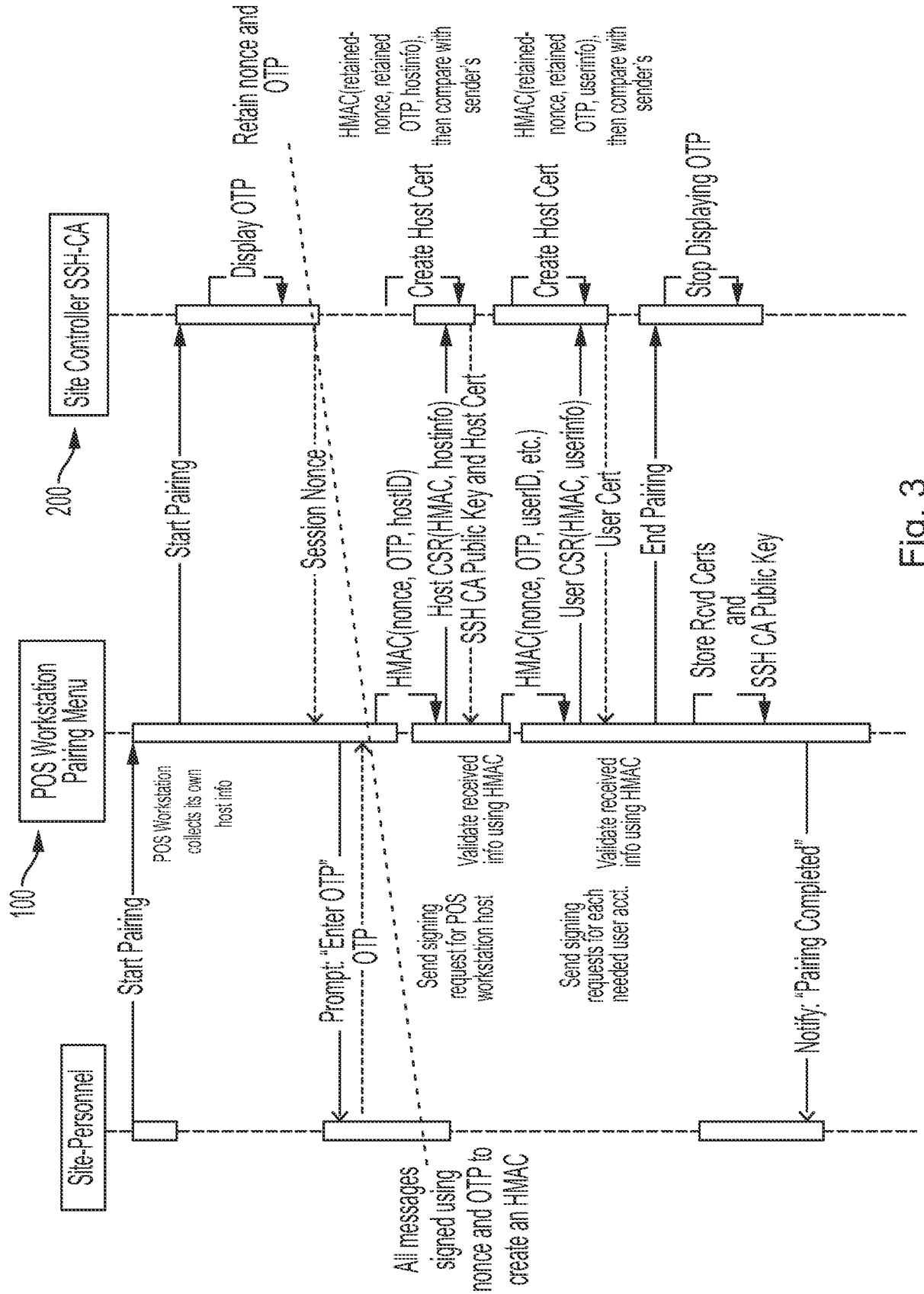

Site-Personnel
POS Workstation Pairing Menu
Site Controller SSH-CA
100
200
Start Pairing
POS Workstation collects its own host info
Start Pairing
Display OTP
Retain nonce and OTP
Session Nonce
Prompt: "Enter OTP"
OTP
Send signing request for POS workstation host
HMAC(nonce, OTP, hostID)
Host CSR(HMAC, hostinfo)
Create Host Cert
HMAC(retained-nonce, retained OTP, hostinfo), then compare with sender's
SSH CA Public Key and Host Cert
Validate received info using HMAC
HMAC(nonce, OTP, userID, etc.)
User CSR(HMAC, userinfo)
Create Host Cert
HMAC(retained-nonce, retained OTP, userinfo), then compare with sender's
User Cert
Send signing requests for each needed user acct.
Validate received info using HMAC
End Pairing
Stop Displaying OTP
Store Rcvd Certs and SSH CA Public Key
Notify: "Pairing Completed"
All messages signed using nonce and OTP to create an HMAC

Fig. 3

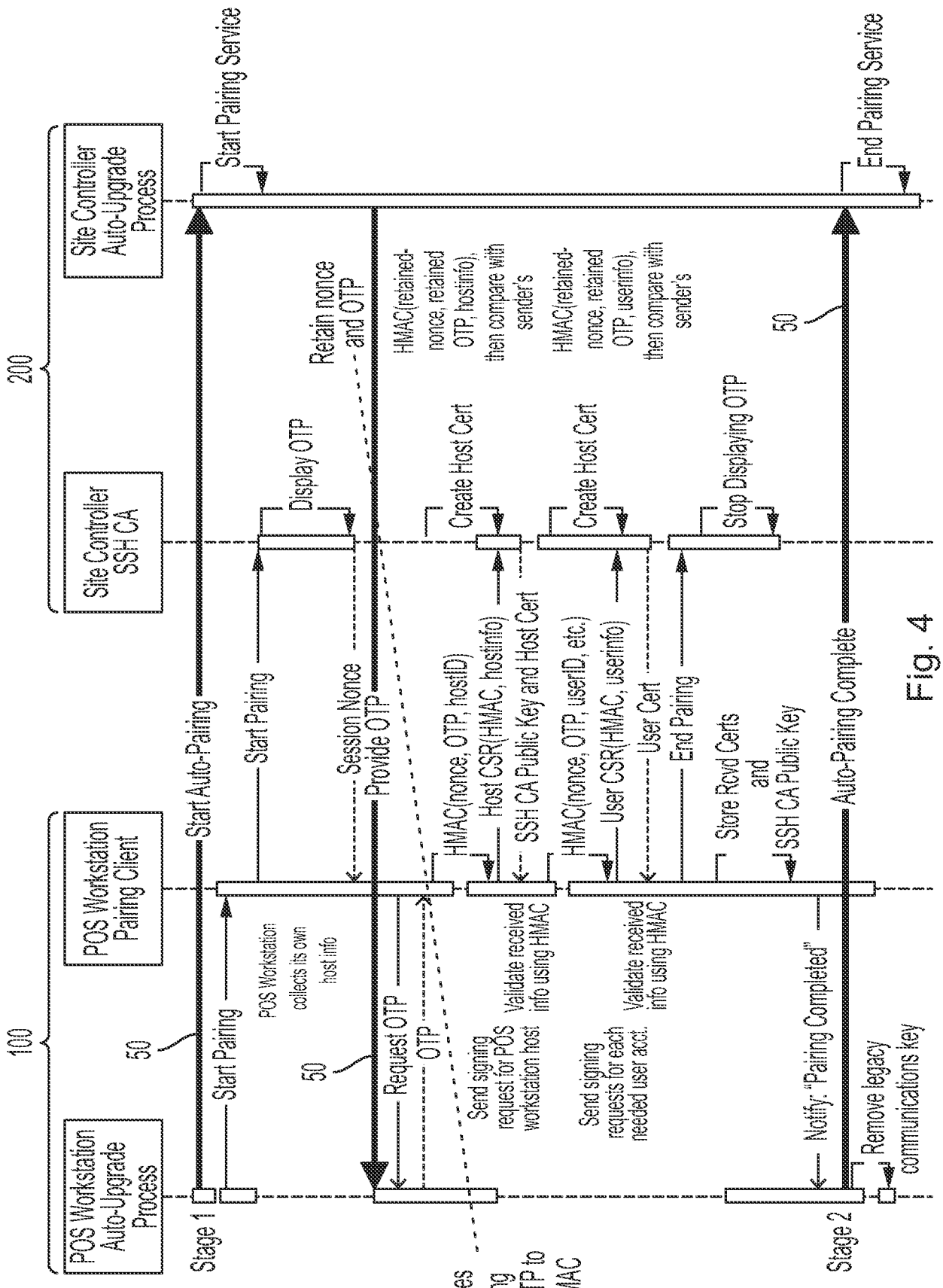

100
200
POS Workstation Auto-Upgrade Process
POS Workstation Pairing Client
Site Controller SSH CA
Site Controller Auto-Upgrade Process
Stage 1
Stage 2
Start Pairing Service
End Pairing Service
Start Auto-Pairing
Start Pairing
POS Workstation collects its own host info
Display OTP
Retain nonce and OTP
Request OTP
OTP
Session Nonce
Provide OTP
HMAC(nonce, OTP, hostID)
Host CSR(HMAC, hostinfo)
Create Host Cert
HMAC(retained-nonce, retained OTP, hostinfo), then compare with sender's
SSH CA Public Key and Host Cert
Validate received info using HMAC
HMAC(nonce, OTP, userID, etc.)
User CSR(HMAC, userinfo)
Create Host Cert
HMAC(retained-nonce, retained OTP, userinfo), then compare with sender's
User Cert
Validate received info using HMAC
End Pairing
Stop Displaying OTP
Store Rcvd Certs and SSH CA Public Key
Auto-Pairing Complete
Notify: "Pairing Completed"
Remove legacy communications key
50
50
50
Send signing request for POS workstation host
Send signing requests for each needed user acct.
All messages signed using nonce and OTP to create an HMAC

Fig. 4

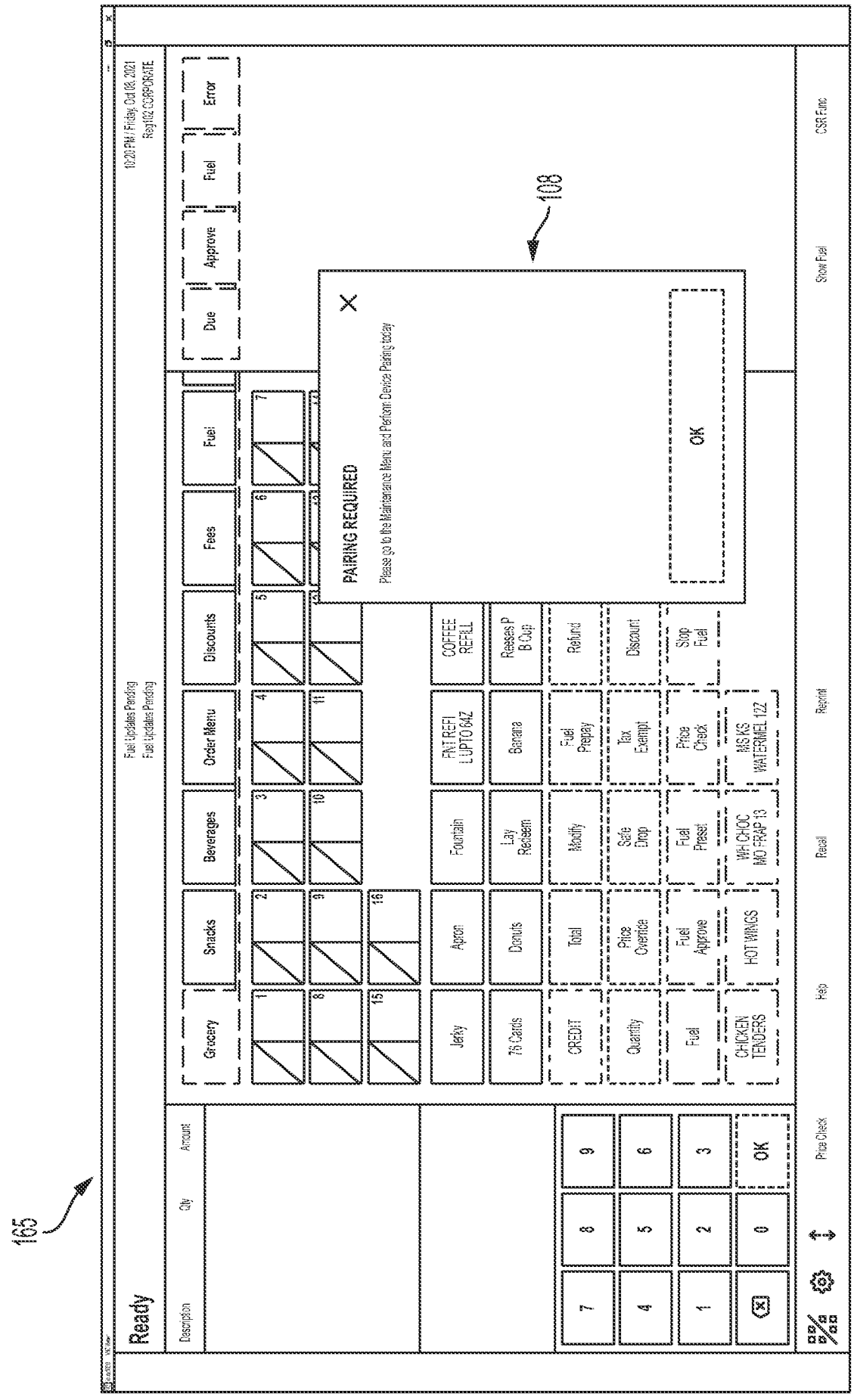

165
Ready
Description
Qty
Amount
Fuel Updates Pending
Fuel Updates Pending
10:20 PM / Friday, Oct 08, 2021
Reg#02 CSR:PORGATE
Grocery
Snacks
Beverages
Order Menu
Discounts
Fees
Fuel
Due
Approve
Fuel
Error
Jerky
Apron
Donuts
Total
Price Override
Fuel Approve
HOT WINGS
Fountain
Lay Redeem
Modify
Safe Drop
Fuel Preset
WH CHOC IMO FRAP 13
PNT REFI L UPTO 64Z
Banana
Fuel Prepay
Tax Exempt
Price Check
MS KS WATERMEL 122
COFFEE REFILL
Reeses P B Cup
Refund
Discount
Stop Fuel
PAIRING REQUIRED
Please go to the Maintenance Menu and Perform Device Pairing today
OK
108
7 Cards
CREDIT
Quantity
Fuel
CHICKEN TENDERS
7
8
9
4
5
6
1
2
3
0
OK
Price Check
Help
Recall
Reprint
Show Fuel
CSR Func

Fig. 5

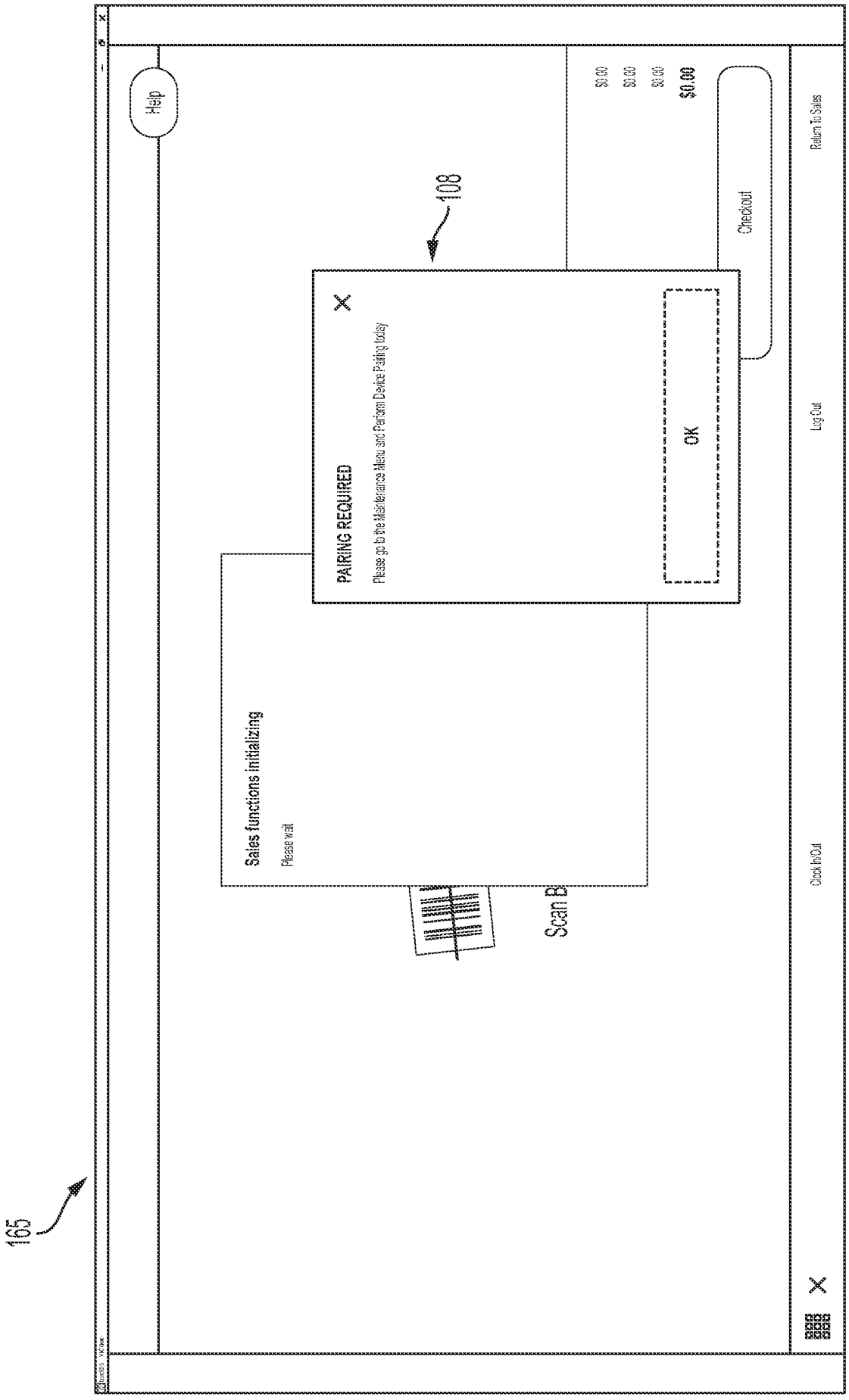

165
Help
108
$0.00
$0.00
$0.00
$0.00
Checkout
Return To Sales
Log Out
Clock In/Out
PAIRING REQUIRED
Please go to the Maintenance Menu and Perform Device Pairing today
OK
Sales functions initializing
Please wait
Scan B

Fig. 6

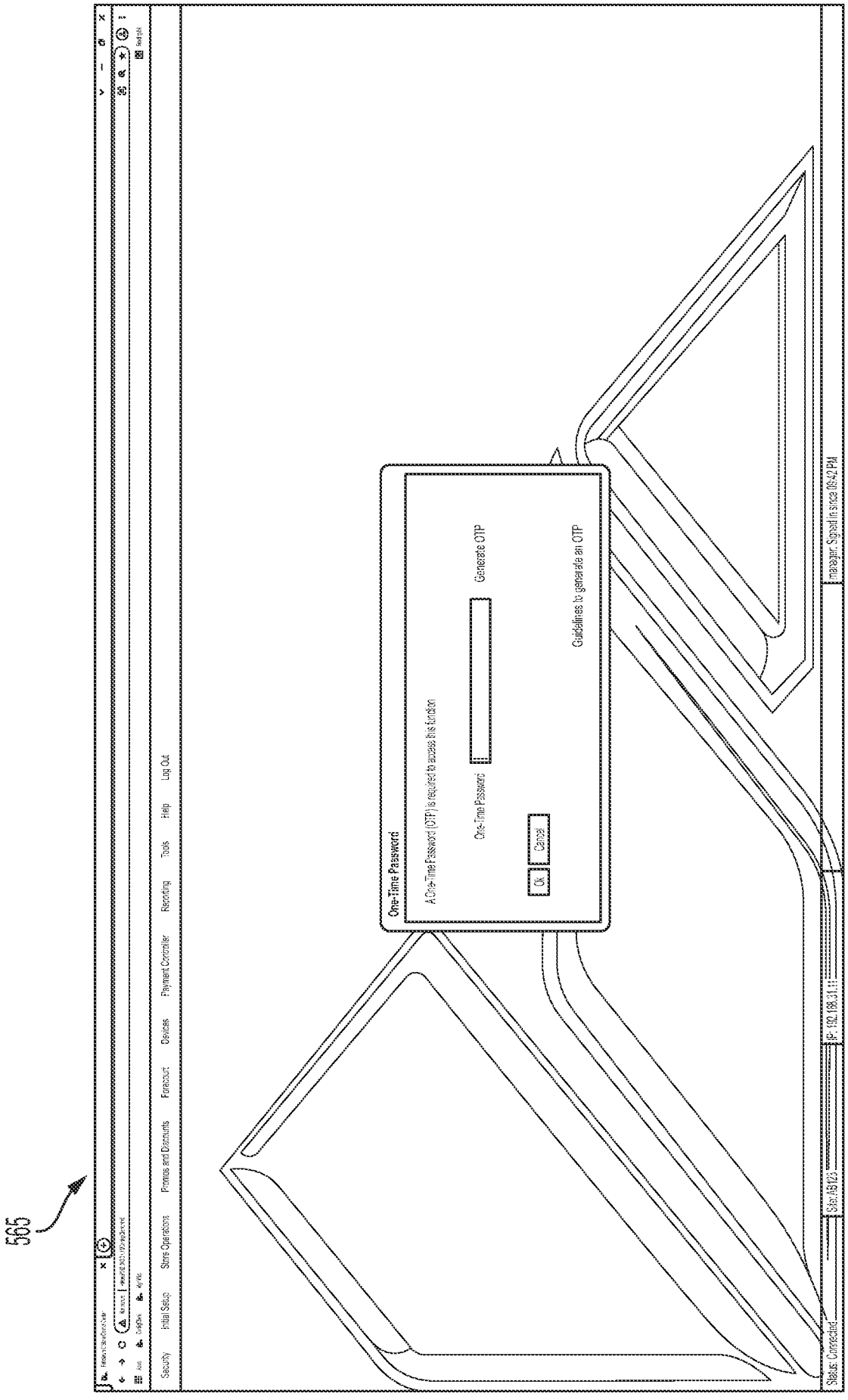

565
Security
Initial Setup
Store Operations
Promos and Discounts
Forecourt
Devices
Payment Controller
Reporting
Tools
Help
Log Out
One-Time Password
A One-Time Password (OTP) is required to access this function
One-Time Password
Generate OTP
Guidelines to generate an OTP
OK
Cancel
Status: Connected
manager: Signed in since 06:42 PM

Fig. 7

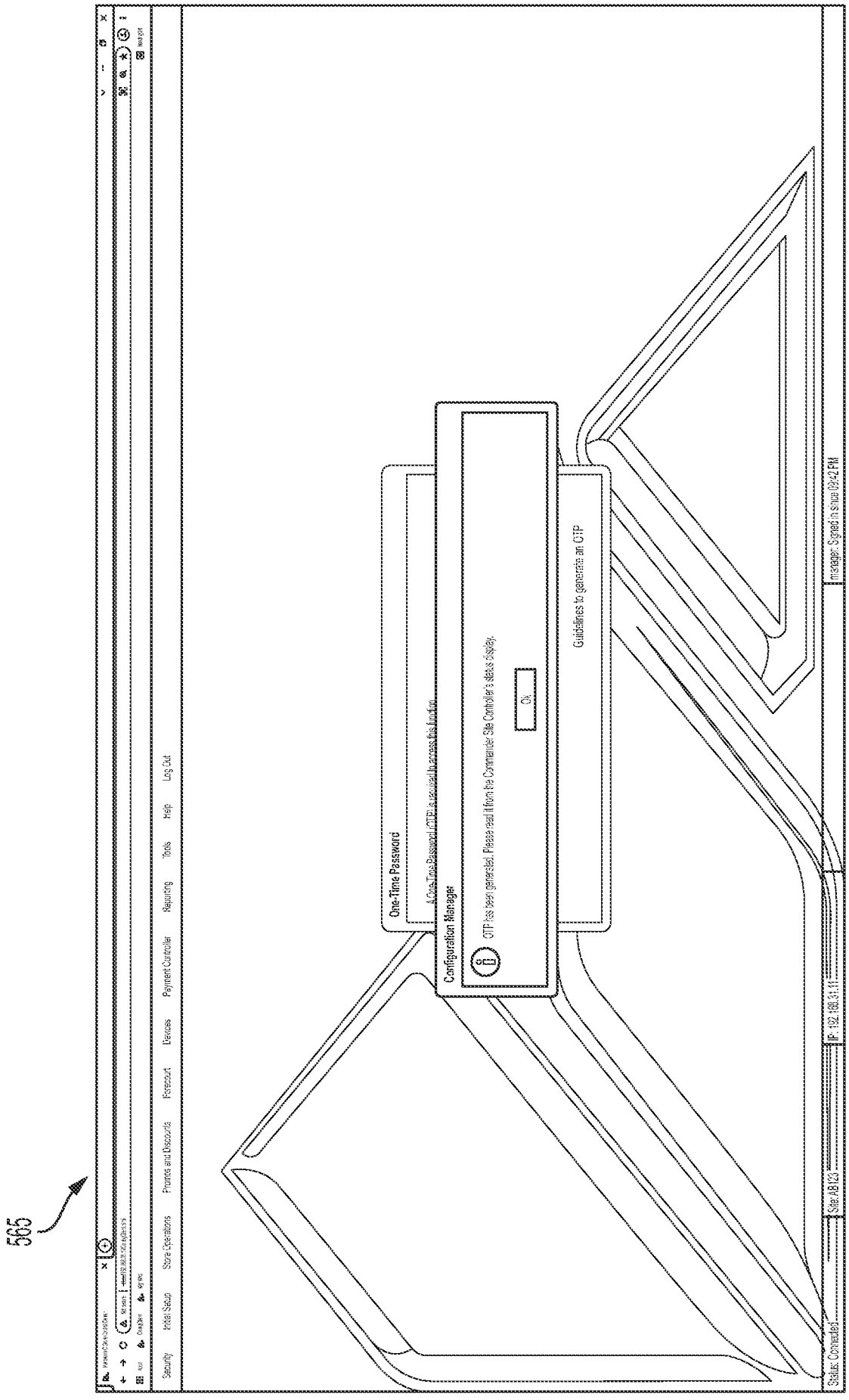

505
Security
Initial Setup
Store Operations
Promos and Discounts
Forecourt
Devices
Payment Controller
Reporting
Tools
Help
Log Out
One-Time Password
A One-Time Password (OTP) is required to access this function.
Configuration Manager
OTP has been generated. Please read it from the Commander Site Controller's status display.
OK
Guidelines to generate an OTP
Status: Connected
Site: AB123
IP: 192.168.31.11
manager: Signed in since 09:42 PM

Fig. 8

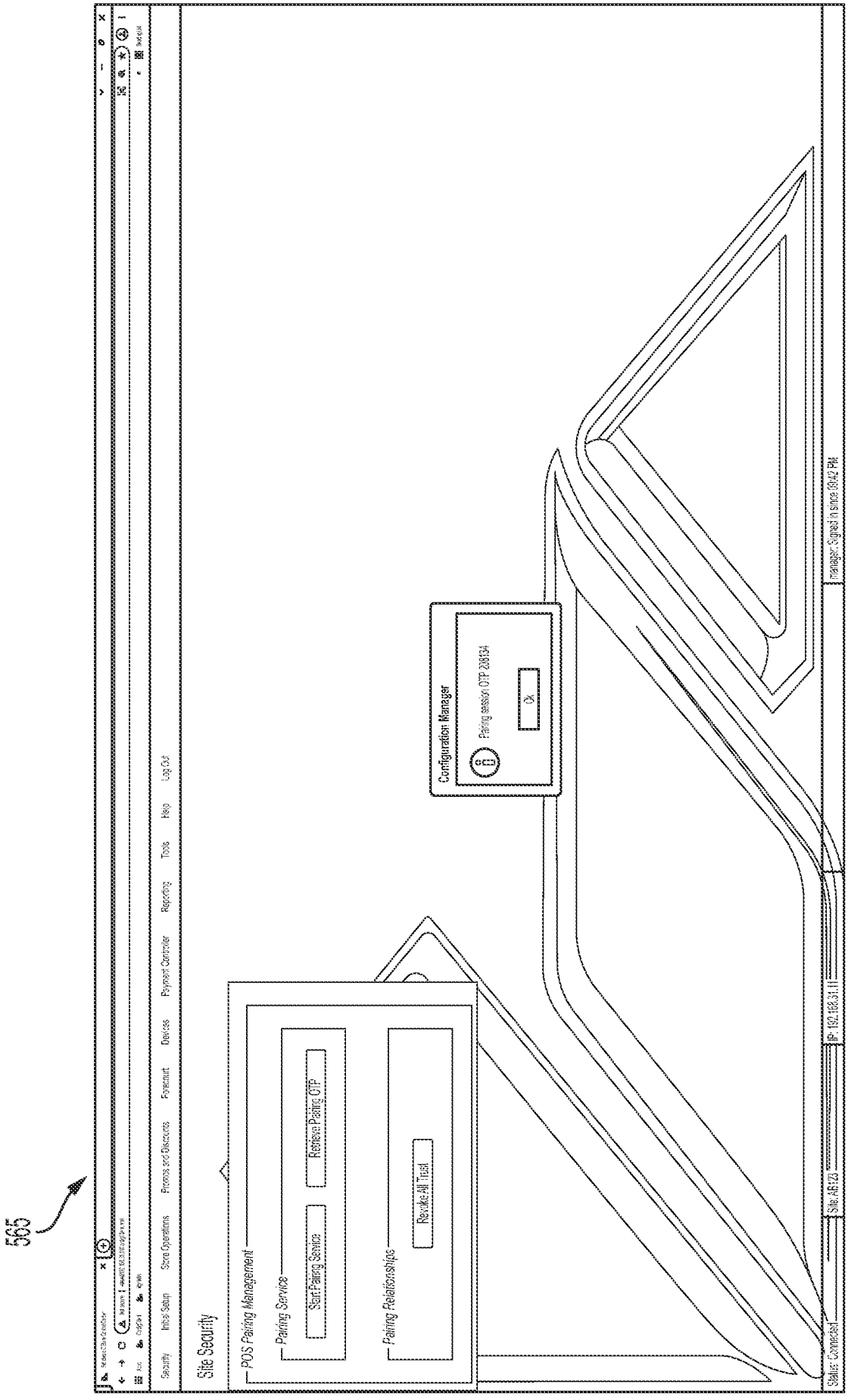

565
Security
Initial Setup
Store Operations
Promos and Discounts
Payment
Devices
Payment Controller
Reporting
Tools
Help
Log Out
Site Security
POS Pairing Management
Pairing Service
Start Pairing Service
Retrieve Pairing OTP
Pairing Relationships
Revoke All Trust
Configuration Manager
Pairing session OTP 208134
Ok
Status: Connected
Site: AB123
IP: 192.168.31.11
manager: Signed in since 09:42 PM

Fig. 9

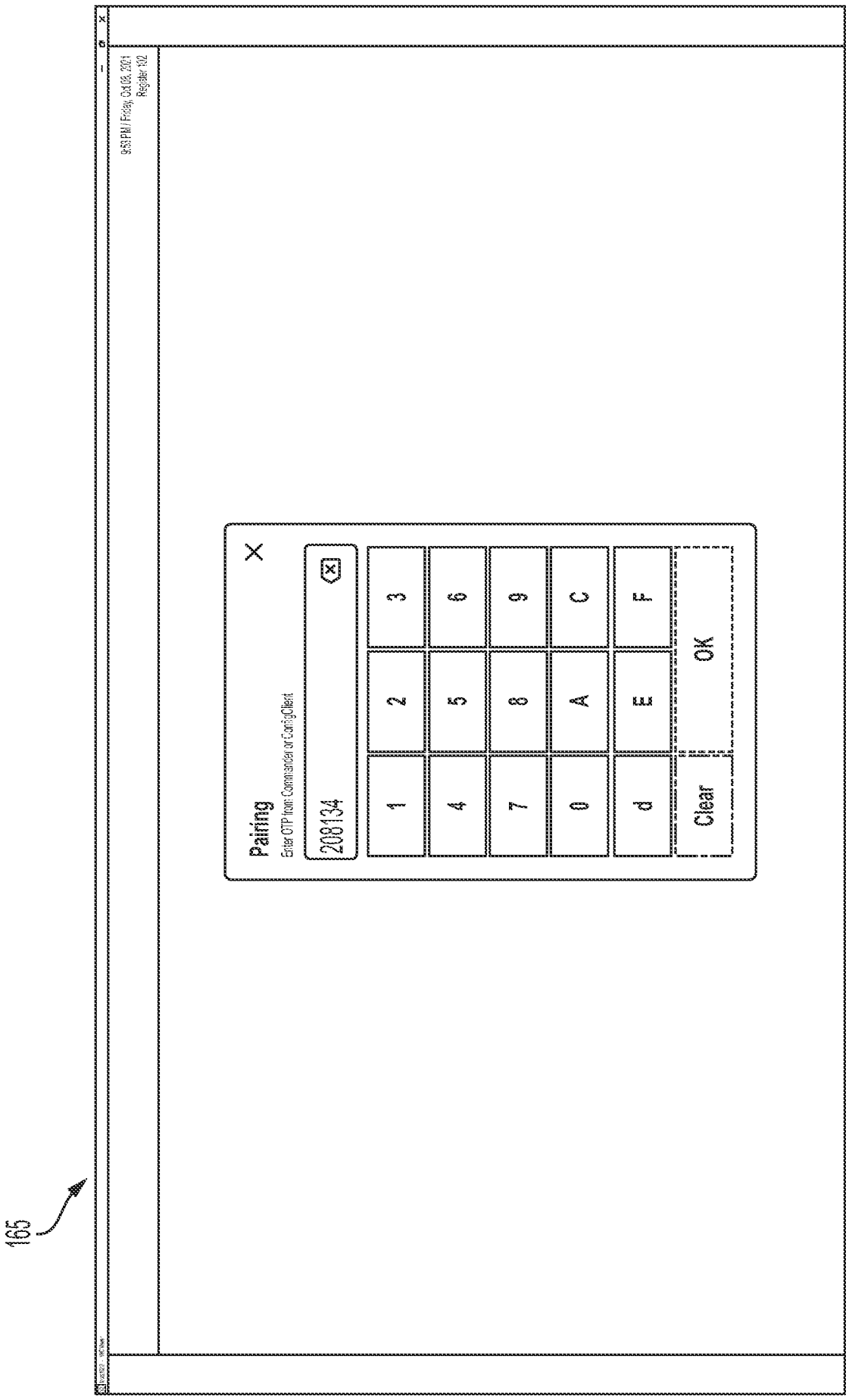

165
9:53 PM | Friday, Oct 08, 2021
Register 192
Pairing
Enter OTP from Commander or ConfigClient
208134
1
2
3
4
5
6
7
8
9
0
A
C
d
E
F
Clear
OK

Fig. 10

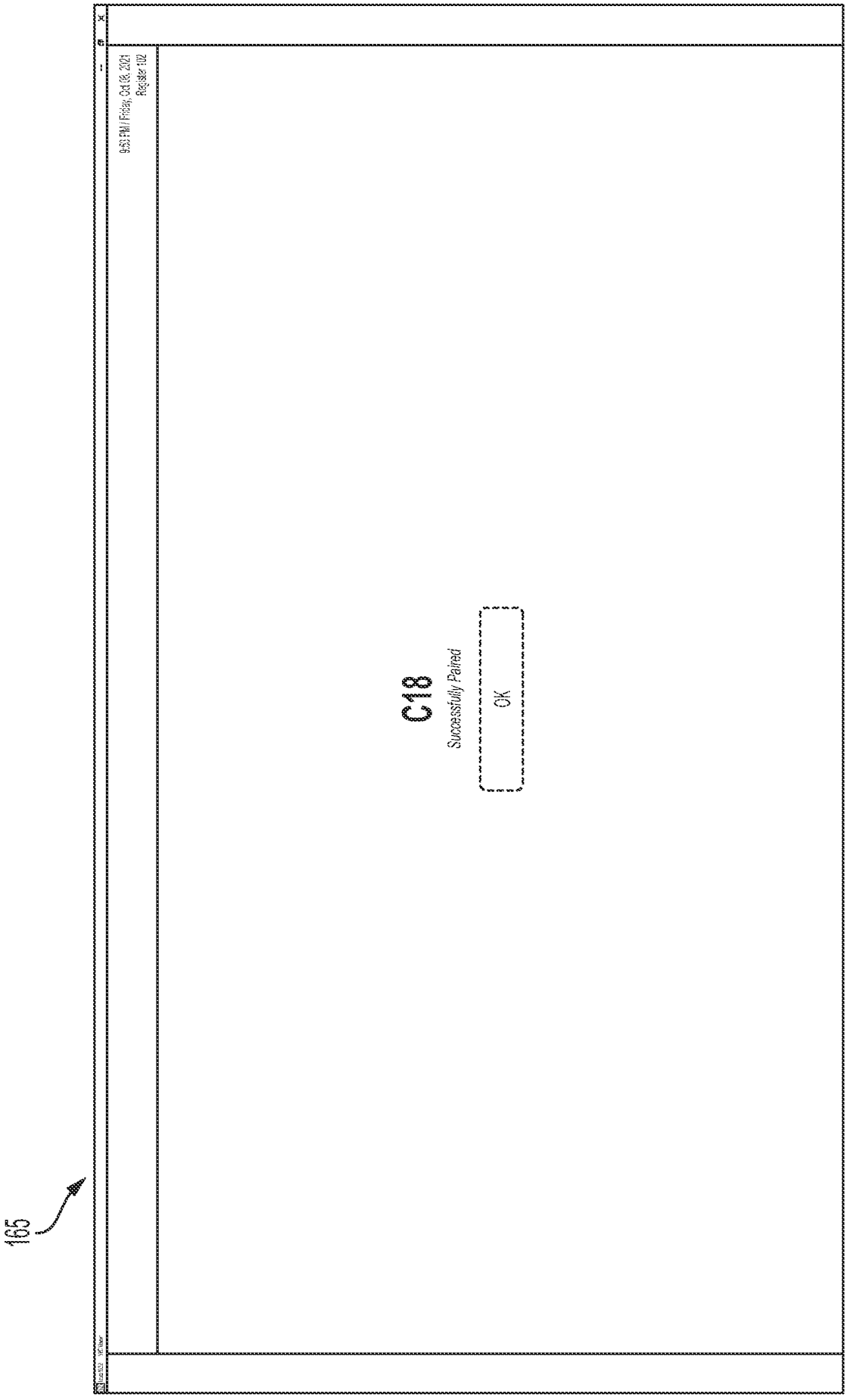

9:50 PM Friday, Oct 08, 2021
Register 102
C18
Successfully Paired
OK
165

Fig. 11

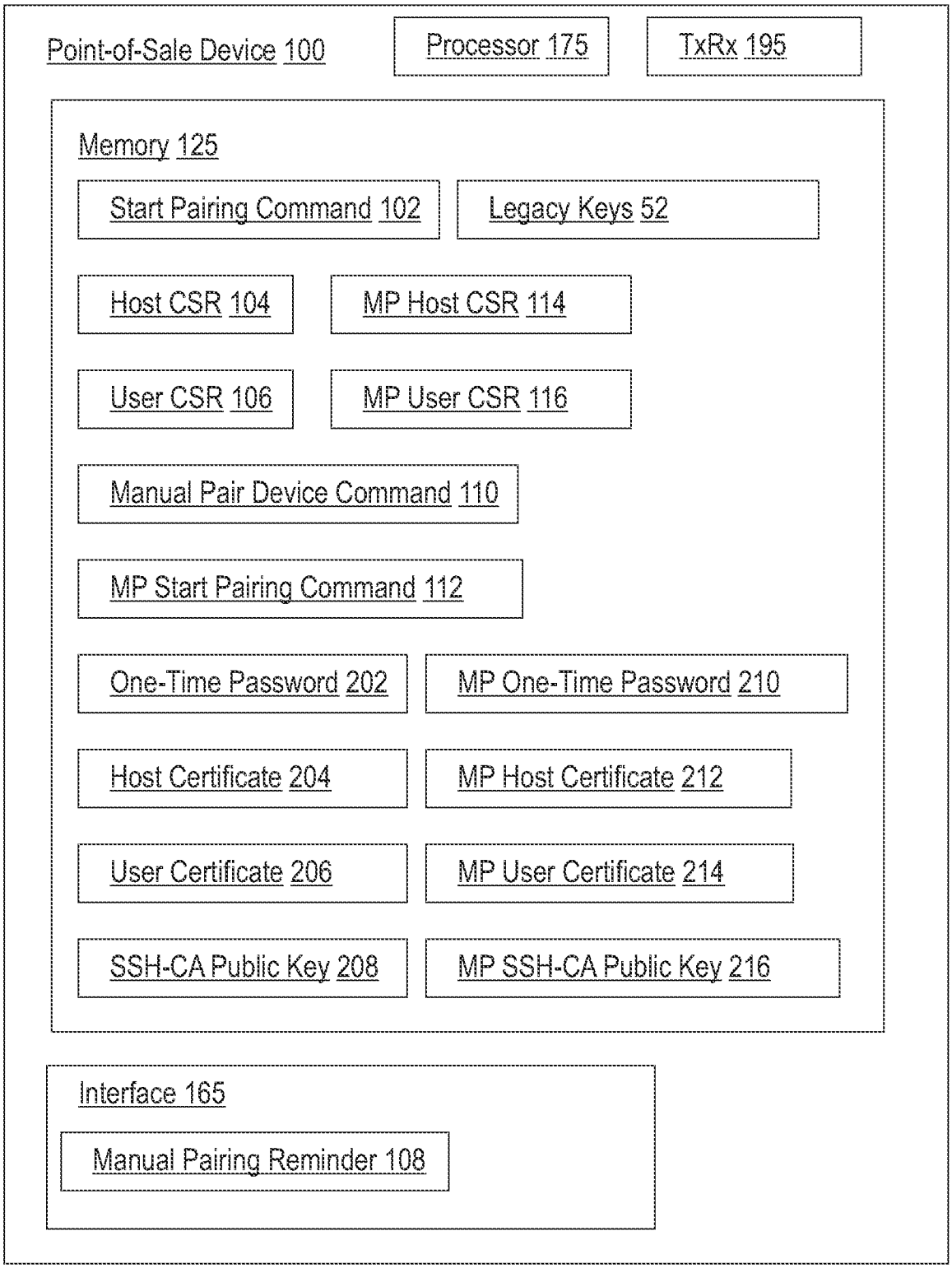

Point-of-Sale Device 100
Processor 175
TxRx 195
Memory 125
Start Pairing Command 102
Legacy Keys 52
Host CSR 104
MP Host CSR 114
User CSR 106
MP User CSR 116
Manual Pair Device Command 110
MP Start Pairing Command 112
One-Time Password 202
MP One-Time Password 210
Host Certificate 204
MP Host Certificate 212
User Certificate 206
MP User Certificate 214
SSH-CA Public Key 208
MP SSH-CA Public Key 216
Interface 165
Manual Pairing Reminder 108

Fig. 12

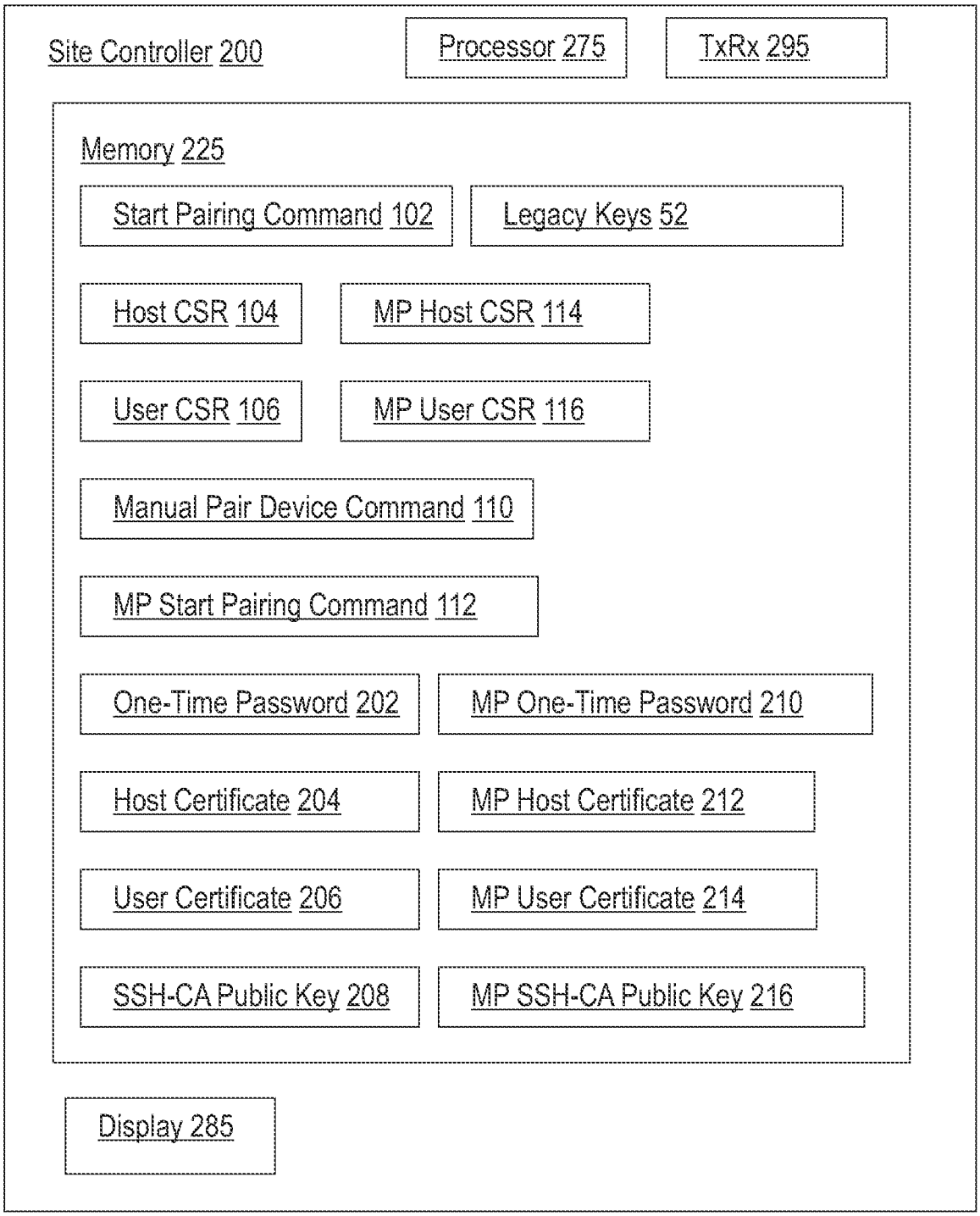

Site Controller 200
Processor 275
TxRx 295
Memory 225
Start Pairing Command 102
Legacy Keys 52
Host CSR 104
MP Host CSR 114
User CSR 106
MP User CSR 116
Manual Pair Device Command 110
MP Start Pairing Command 112
One-Time Password 202
MP One-Time Password 210
Host Certificate 204
MP Host Certificate 212
User Certificate 206
MP User Certificate 214
SSH-CA Public Key 208
MP SSH-CA Public Key 216
Display 285

Fig. 13

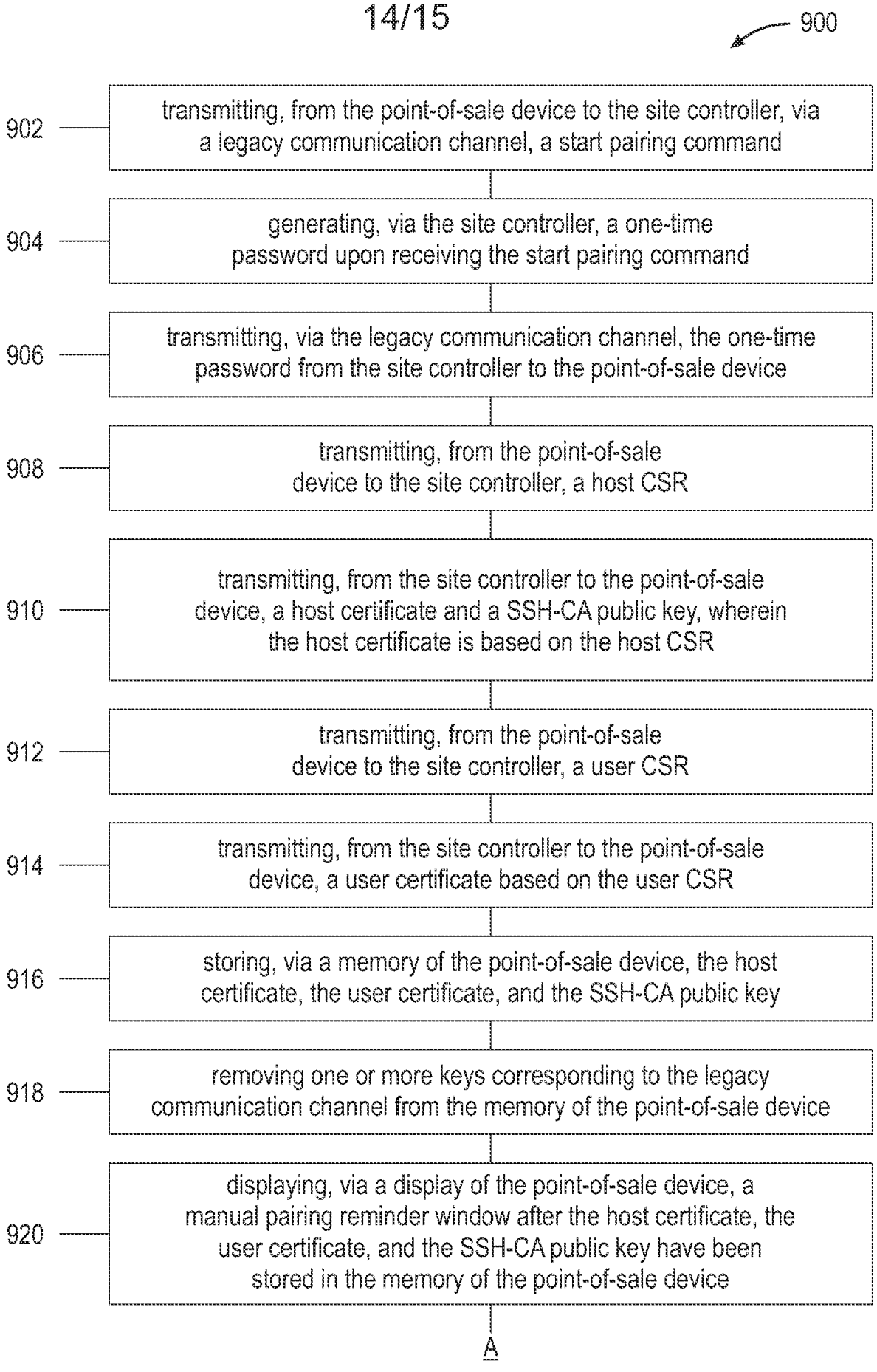

900
902
transmitting, from the point-of-sale device to the site controller, via a legacy communication channel, a start pairing command
904
generating, via the site controller, a one-time password upon receiving the start pairing command
906
transmitting, via the legacy communication channel, the one-time password from the site controller to the point-of-sale device
908
transmitting, from the point-of-sale device to the site controller, a host CSR
910
transmitting, from the site controller to the point-of-sale device, a host certificate and a SSH-CA public key, wherein the host certificate is based on the host CSR
912
transmitting, from the point-of-sale device to the site controller, a user CSR
914
transmitting, from the site controller to the point-of-sale device, a user certificate based on the user CSR
916
storing, via a memory of the point-of-sale device, the host certificate, the user certificate, and the SSH-CA public key
918
removing one or more keys corresponding to the legacy communication channel from the memory of the point-of-sale device
920
displaying, via a display of the point-of-sale device, a manual pairing reminder window after the host certificate, the user certificate, and the SSH-CA public key have been stored in the memory of the point-of-sale device
A

Fig. 14

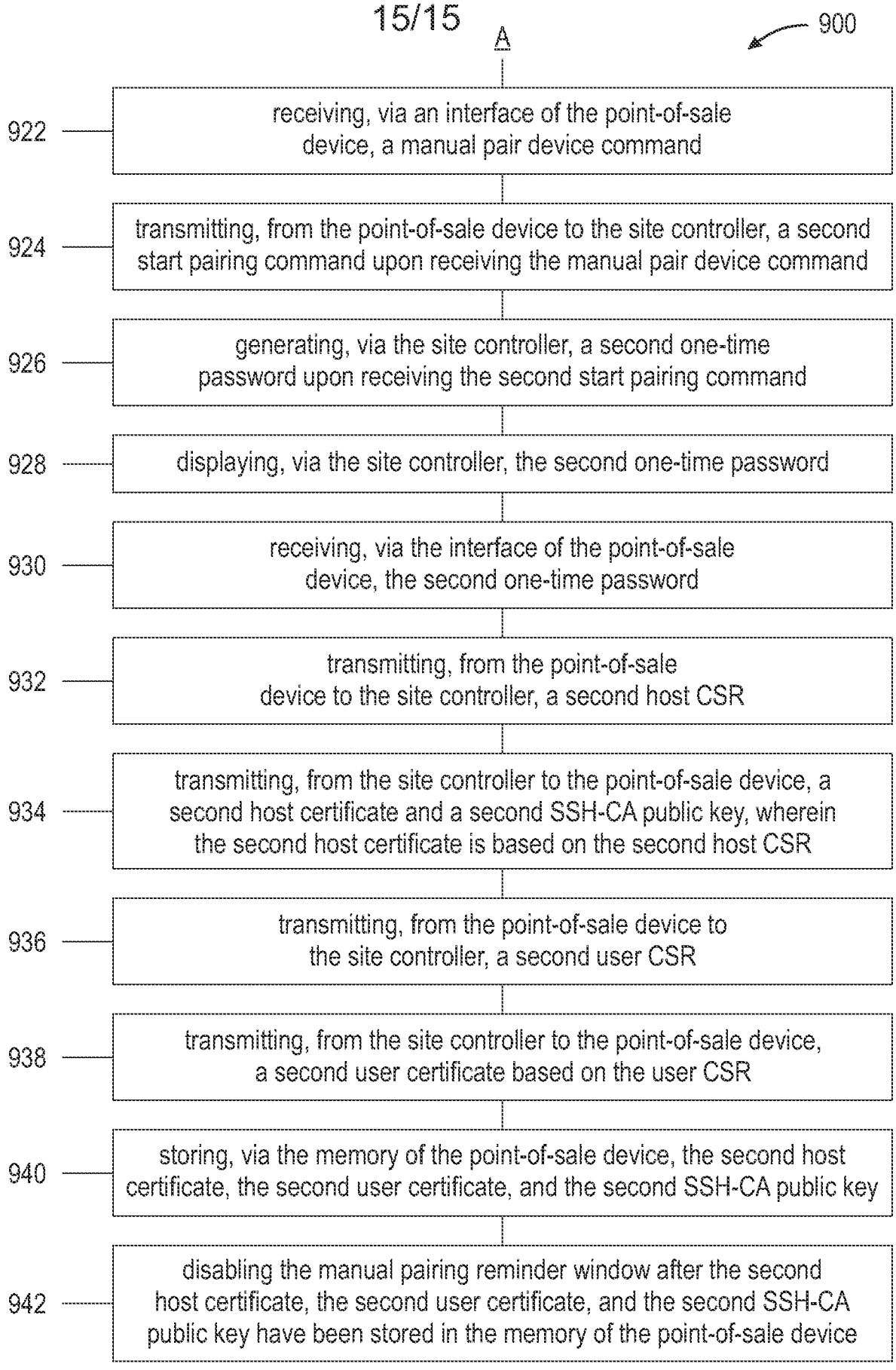

A
900
922
receiving, via an interface of the point-of-sale device, a manual pair device command
924
transmitting, from the point-of-sale device to the site controller, a second start pairing command upon receiving the manual pair device command
926
generating, via the site controller, a second one-time password upon receiving the second start pairing command
928
displaying, via the site controller, the second one-time password
930
receiving, via the interface of the point-of-sale device, the second one-time password
932
transmitting, from the point-of-sale device to the site controller, a second host CSR
934
transmitting, from the site controller to the point-of-sale device, a second host certificate and a second SSH-CA public key, wherein the second host certificate is based on the second host CSR
936
transmitting, from the point-of-sale device to the site controller, a second user CSR
938
transmitting, from the site controller to the point-of-sale device, a second user certificate based on the user CSR
940
storing, via the memory of the point-of-sale device, the second host certificate, the second user certificate, and the second SSH-CA public key
942
disabling the manual pairing reminder window after the second host certificate, the second user certificate, and the second SSH-CA public key have been stored in the memory of the point-of-sale device

Fig. 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US22/78696

A. CLASSIFICATION OF SUBJECT MATTER

IPC - INV. G06Q 20/16; G06Q 20/20; G06Q 20/38; H04L 9/32 (2022.01)
ADD. G06F 21/31; G06Q 20/10; G06Q 20/18; G06Q 20/32; G06Q 20/34; G06Q 20/40 (2022.01)

CPC - INV. G06Q 20/16; G06Q 20/20; G06Q 20/38215; H04L 9/3263
ADD. G06F 21/31; G06Q 20/105; G06Q 20/18; G06Q 20/32; G06Q 20/34; G06Q 20/405

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)
See Search History document

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

Electronic database consulted during the international search (name of database and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2021/0279703 A1 (FISERV, INC.) 09 September 2021; Entire document	1-20
A	WO 2020/082164 A1 (NYMI INC.) 30 April 2020; Entire document	1-20
A	US 2016/0125376 A1 (CLOVER NETWORK, INC.) 05 May 2016; Entire document	1-20
A	US 2008/0183629 A1 (KAUSIK, B) 31 July 2008; Entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ 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
"D" document cited by the applicant in the international application
"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
05 January 2023 (05.01.2023)	FEB 03 2023
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas Telephone No. PCT Helpdesk: 571-272-4300