Technical Disclosure Commons

InVue Defensive Publications | Defensive Publications Series

August 11, 2017

ACCESS AUTHORIZATION SYSTEMS AND DEVICES FOR RETAIL MERCHANDISING SYSTEMS

InVue Security Products Inc.

Follow this and additional works at: http://www.tdcommons.org/invue

Recommended Citation

InVue Security Products Inc., "ACCESS AUTHORIZATION SYSTEMS AND DEVICES FOR RETAIL MERCHANDISING SYSTEMS", Technical Disclosure Commons, (August 11, 2017)
http://www.tdcommons.org/invue/15

This work is licensed under a Creative Commons Attribution 4.0 License.

This Article is brought to you for free and open access by the Defensive Publications Series at Technical Disclosure Commons. It has been accepted for inclusion in InVue Defensive Publications by an authorized administrator of Technical Disclosure Commons.

ACCESS AUTHORIZATION SYSTEMS AND DEVICES FOR RETAIL MERCHANDISING SYSTEMS

FIELD OF THE INVENTION

[0001] Embodiments of the present invention relate generally to access authorization systems and devices for electronic retail merchandising systems. More particularly, embodiments of the present invention relate to access authorization systems and devices used to allow and/or deny access to portable electronic devices associated with retail merchandising systems.

BACKGROUND OF THE INVENTION

[0002] Retail merchandisers often supply their stores and merchandising systems with portable electronic devices, such as handheld devices, tablets, and laptop computers. The handheld devices, tablets, and laptop computers generally assist employees, managers and store associates in helping customers with their shopping experience. For instance, the portable electronic devices provide employees, managers and store associates with increased mobility within the store thereby being readily available to assist customers. The associate may use the portable electronic device for tasks such as displaying a layout of the store, locating merchandise, checking on the price of an item, or accessing information regarding a product that the customer is buying. In some stores, portable electronic devices may also be used to assist customers with the final financial transaction associated with a purchase. Portable electronic devices may also be used to provide retail merchandisers with data associated with product inventory and sales. Notably, the use of portable electronic devices in retail stores potentially maximizes the likelihood of a sale by increasing the readiness for assisting customers on demand, as well as providing organized access of product data. Additionally, restaurants may use portable electronic devices at a table for ordering or entertainment for patrons, and hospitals may use portable electronic devices to allow doctors and nurses mobile access to patient health records.

BRIEF SUMMARY OF THE DRAWINGS

[0003] FIG. 1 illustrates an access authorization system and device according to one embodiment of the present invention.

[0004] FIG. 2 illustrates an access transfer device according to one embodiment.

[0005] FIG. 3 illustrates a programmable electronic key according to one embodiment.

[0006] FIG. 4 illustrates an access transfer device and programmable electronic key in communication with a remote device via a cloud according to one embodiment.

[0007] FIG. 5 illustrates a plurality of programmable electronic keys with different authorization levels according to one embodiment.

[0008] FIG. 6 illustrates an access authorization system and device according to another embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0009] Embodiments of the present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which various embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

[0010] Referring now to the accompanying figures wherein identical reference numerals denote the same elements throughout the various views, embodiments of a retail merchandising system access authorization device according to the present invention for providing authorized access to portable electronic devices associated with the merchandising system. The portable

electronic devices may be any item, including any number of consumer electronics products (e.g. hand-held device, cellular phone, smart phone, tablet, laptop computer, etc.).

[0011] According to some embodiments, the access authorization systems and devices described herein may be operable for validating authorized access to the merchandising system of a retailer. The access authorization systems and devices may also permit categorized individual and/or multi-user access to retail data and/or portable electronic devices that may be associated with the retail merchandising system. Additionally, the access authorization systems and devices may maintain the readiness of an employee/manager/sales associate to assist customers on demand while minimizing the potential for cross-contamination and/or misuse of the portable electronic device among employees/managers/sales associates. The access authorization systems and devices detailed herein may be suitable for validating authorized access of a portable electronic device for a variety of uses, such as in a residential or commercial environment, and are not intended to be limited for use only as an access authorization system for a merchandising retailer.

[0012] In an exemplary embodiment as shown FIG. 1, an access authorization system 10 may include one or more programmable electronic keys 12, one or more portable electronic devices 14, a programming or authorization station 16, and one or more access transfer devices 18. The programmable electronic key 12 and the one or more access transfer devices 18 may be configured to provide authorized access to the one or more portable electronic devices. The programming or authorization station 16 is operable for programming the electronic key 12 and the access transfer device 18 with a security code, which is also referred to herein as a Security Disarm Code (SDC), described in further detail below. Additionally, embodiments of the access authorization system 10 may also include an optional charging station 19 that is operable for initially charging and/or subsequently recharging a power source that may be disposed within the programmable electronic key 12.

[0013] According to an exemplary embodiment, as shown in Fig. 2, the access transfer device 18 may include an adapter cord 21 operably connected thereto. The adapter cord 21 may include a connector 23 (e.g., a USB or like plug) operably connected at a free end thereof. The connector 23 may be configured to releasably engage a corresponding input port on at least one

of the portable electronic devices 14. The access transfer device 18 may also include an access transfer port 15. The access transfer port 15 may be configured to facilitate communication with the programmable electronic key 12. As mentioned briefly above and as explained in further detail below, the access transfer device 18 may be configured to be programmed by the programmable electronic key 12 with data. In other embodiments, the access transfer device 18 may be used to facilitate communication between the electronic key 12 and the portable electronic device 14 and may not store data for providing access to the portable electronic device 14. The access transfer device 18 may be connected to the portable electronic device 14 by a USB connector 23 and communicate via a USB communication protocol, or the access transfer device 18 and portable electronic device 14 may wirelessly communicate such as via Bluetooth or Wi-Fi communication. The access transfer device 18 may be operable for facilitating authorized access to the portable electronic devices 14 and/or the merchandising system 26 of a retailer. For example, rather than inputting a password, a user may be provided access for use of the portable electronic device 14 when an authorized electronic key 12 is presented to the access transfer device 18. The user may be granted full access to the portable electronic device 14 and all of its functionality, or the user may be granted partial access to particular functions or applications on the portable electronic device 14. In some instances, authorized information and/or applications may be automatically provided to the user when an authorized programmable electronic key 12 is presented to the access transfer device 18.

[0014] In one embodiment, the portable electronic device 14 may be a hand-held device, cellular phone, smart phone, tablet, laptop computer, or other similar device. Generally, portable electronic devices 14 such as hand-held devices, cellular phones, smart phones, tablets, laptop computers, or the like include input ports, such as for receiving a power connector or an auxiliary device connector. The connector 23 (e.g., a USB or like plug) of the access transfer device 18 may be configured to releasably engage a corresponding input port on the portable electronic device 14.

[0015] Embodiments of the access authorization system 10 may further include one or more programmable electronic keys 12 configured to communicate with one or more of the access transfer devices 18. In some embodiments, the programmable electronic key 12 may be similar

to the IR2 and IR3 keys manufactured by InVue Security Products Inc. In some embodiments, the programmable electronic key 12 may be similar to that disclosed in U.S. Patent Appl. No. 13/222,225, entitled Electronic Key for Merchandise Security Device and filed on August 31, 2011; and International Publication No. WO 2016/109281, entitled Merchandise Display Security Systems and Methods and filed on December 21, 2015, the contents of which are incorporated by reference herein. The programmable electronic keys 12 may be programmed to transmit data to the access transfer devices 18 and/or portable electronic devices 14 for allowing or denying access to the at least one or more portable electronic devices 14. The data may be generated by an electrical, optical, acoustical or magnetic source, and may include a security code and/or serial number. In some embodiments, the data is generically referred to herein as a Security Disarm Code (SDC). The SDC may be predetermined by the manufacturer of the access transfer devices 18, or alternatively, may be selected by the retailer at a particular retail location. In some embodiments, the SDC may be randomly generated and unknown to all persons, or alternatively, may be made known only to authorized persons. Accordingly, an unauthorized person without access to the SDC or means to determine the SDC cannot program a duplicate key with the same SDC.

[0016] Furthermore, in some embodiments, the programmable electronic keys 12 may be readily reprogrammed by the retailer with a different SDC in the event that one of the programmable electronic keys 12 is lost or stolen. In the event that a programmable electronic key 12 is lost or stolen, the replacement programmable electronic keys 12 may be programmed with a randomly generated SDC that may be unique and unknown to any individual. For example, the programmable electronic key 12 and access transfer device 18 may each be programmed with the same SDC into a respective permanent memory. The programmable electronic key 12 may be provisioned with a single-use (i.e., non-rechargeable) power source, such as a conventional or extended-life battery, or alternatively, the programmable electronic key 12 may be provisioned with a multiple-use (i.e. rechargeable) power source, such as a conventional capacitor or rechargeable battery. In either instance, the power source may be permanent, semi-permanent (i.e., replaceable), or rechargeable, as desired. In the latter instance, charging station 19 may be provided to initially charge and/or to subsequently recharge the

power source provided within the programmable electronic key 12.

[0017] In other embodiments, the SDC may be a predetermined (i.e. "factory preset") security code, a manually input security code, or a security code that is randomly generated by the logic control circuit. For example, in one embodiment, the logic control circuit further comprises a random number generator for producing the unique SDC. In some embodiments, the programmable electronic key 12 may be provided with only a transient memory, such that the SDC must be programmed (or reprogrammed) at predetermined time intervals. For example, in one embodiment, programming station 16 may be provided to initially program and/or to subsequently reprogram the SDC into the programmable electronic key 12.

[0018] In one embodiment, as shown in Fig. 3, the programmable electronic key 12 may include a housing 123 configured to contain the internal components of the programmable electronic key 12 such as, including without limitation, a logic control circuit, memory, communication system and battery. The programmable electronic key 12 may include a transfer probe 125 located at an end of the housing 123 wherein the transfer probe may be configured to facilitate communication with the programming station 16 and for transferring data and/or power to the access transfer device 18 and/or portable electronic devices 14. In some embodiments, the programmable electronic key 12 may include a control button 122. The control button 122 may be configured to operatively control certain operations of the logic control circuit, memory, communication system, and in particular, the transmission of data and/or power.

[0019] In some embodiments, and as noted above, the programmable electronic key 12 of the access authorization system 10 may be configured to be programmed with a unique SDC by the programming station 16. In an exemplary embodiment, the programming station 16 suitable for use with the present invention may function in a similar manner to that shown and described in detail in the commonly owned United States Patent No. 7,737,844 entitled Programming Station For A Security System For Protecting Merchandise, the disclosure of which is incorporated herein by reference in its entirety. The programming station 16 may include a programming port 46. The programming port 46 is configured to facilitate communication with the programmable electronic key 12. In one embodiment, the programming station 16 may also be configured to contain a logic control circuit that generates the SDC, the memory that stores the SDC, and a

communications system for communicating the SDC to the programmable electronic key 12 (e.g., wirelessly). In use, transfer probe 125 of the programmable electronic key 12 is presented adjacent or proximate to the programming port 46 of the programming station where the logic control circuit then generates the SDC. A series of visual indicators, for example light-emitting diodes (LEDs) may also be provided on an exterior of the programming station 16 for indicating that the programming station 16 is operating. Programming station 16 may further be provided with an access mechanism for preventing use of the programming station 16 by unauthorized persons. For example, the programming station may include a keypad 44. An authorized user may input a code in the key pad 44 that allows the programming station 16 to generate a SDC for communicating to the programmable electronic key 12. The programmable electronic key 12 may then be further operable to activate the access transfer device 18 by communicating the data to the access transfer device 18 thereby defining authorized access to the portable electronic device 14 and/or controlling the availability of data and other retailer information contained on the portable electronic device 14 or stored in the merchandising system 26 of a retailer.

[0020] In a particular embodiment, the logic control circuit of the programming station 16 performs an electronic exchange of data with the logic control circuit of the programmable electronic key 12, commonly referred to as a "handshake communication protocol." The handshake communication protocol determines whether the programmable electronic key 12 is an authorized key that has not been programmed previously (e.g., a "new" key), or is an authorized key that is being presented to the programming station 16 a subsequent time to refresh the SDC. In the event that the handshake communication protocol fails, the programming station 16 will not provide the SDC to the unauthorized device attempting to obtain the SDC. When the handshake communication protocol succeeds, the programming station 16 permits the SDC to be transmitted by the programmable electronic key 12. As will be readily apparent to those skilled in the art, the SDC may be transmitted from the programming station 16 to the programmable electronic key 12 by any suitable means, including without limitation, wireless, electrical contacts or electromechanical, electromagnetic or magnetic conductors, as desired. Moreover, in other cases the programming station 16 may simply provide the SDC to the programmable electronic key 12 without first initiating any handshake communication protocol. In one

embodiment, a series of visual indicators, for example light-emitting diodes (LEDs) may also be provided on an exterior of the programmable electronic key 12 for indicating that the programmable electronic key 12 is operating.

[0021] In some embodiments, the "handshake communication protocol" may be performed between the programmable electronic key 12 and the access transfer device 18 and/or the portable electronic device 14. In one embodiment, a user, such as an employee, retail manager or sales associate presents the transfer probe 125 of the programmable electronic key 12 proximate or adjacent to an access transfer port 15 of the access transfer device 18, wherein at which time, the handshake communication protocol is transmitted/received between the programmable electronic key 12 and the access transfer device 18 and/or the portable electronic device 14. If the handshake communication protocol is successful and the employee, retail manager or sales associate is an authorized user of the portable electronic device 14, wherein the previously programmed electronic key 12 matches the SDC code of the assigned portable electronic device 14, the authorized user may then be allowed access to the portable electronic device 14 and/or allowed access to a pre-identified portion of the merchandising system 26 of a retailer. On the other hand, if the handshake communication protocol is unsuccessful and the employee, retail manager or sales associate is not identified, via the electronic communication exchange of data between the programmable electronic key 12 and the access transfer device 18 and/or the portable electronic device 14, as an authorized user of the portable electronic device 14, the portable electronic device 14 may then remain inaccessible to the employee, retail manager or sales associate. In other embodiments, access may be authorized to the portable electronic device 14 when the SDC matches and power is transferred to the portable electronic device 14. It is understood that various information and codes may be exchanged in order to perform the desired access functions. For example, in one embodiment, the data communication exchange may include a serial number and/or a security code. In some embodiments, a handshake communication protocol may be optional, and access may be provided to the portable electronic device 14 if a security code or other data exchanged between the electronic key 12 and the portable electronic device match.

[0022] In contrast to conventional systems where an authorized user having an alpha-

numeric or similar password that is physically entered to gain access to a portable electronic device 14, in one embodiment of the present invention, an authorized user may gain access to the portable electronic device 14 through an electronic communication exchange of data between the programmable electronic key 12 and the access transfer device 18 and/or the portable electronic device 14. Hence, the need to memorize passwords or access codes or the potential to lose or share access codes is minimized, and access to proprietary retail information may be more secure. Additionally, where the electronic communication exchange of data between the programmable electronic key 12 and the access transfer device 18 and/or the portable electronic device 14 is wireless, this exchange removes the requirement of physical contact and minimizes wear and tear between the programmable electronic key 12 and the access transfer device 18.

[0023] In some embodiments, each one of the portable electronic devices 14 may include a serial number. One or more serial numbers of each portable electronic device 14 may be programmed in one or more electronic keys 12 by the retailer to correlate with a unique security access. This allows for greater flexibility in programming the programmable electronic keys 12 in that specific programmable electronic keys 12 may be assigned to particular portable electronic devices 14, zones within the retail store, employee/manager/sales associate, and/or data accessible through a retail merchandising system. In some embodiments, the programmable electronic key 12 may be operable to initially program and/or to subsequently reprogram the access transfer device 18 and/or the portable electronic device 14 with the SDC and/or other data. For example, and as shown in Fig. 4, at an initial setup, the programmable electronic key 12 may be used to initially map the serial numbers for particular portable electronic devices 14. In this regard, the programmable electronic key 12 may be used to communicate with the retail merchandising system 26 to obtain the serial number of each portable electronic device 14. A user (e.g., # 1234) initiating the initial setup may also prescribe a specified operable location for a portable electronic device 14 within the retail store, or may provide a description for each portable electronic devices 14 (e.g., SN # 123 = portable electronic device 14 #1). The programmable electronic key 12 may then be presented to the access transfer device 18 for communication with the retail merchandising system 26 for accumulating all of the information contained therein and/or previously defined information or portable electronic

devices 14 specified for access from the retailer contained therein. Thus, the retail merchandising system 26 may map each of the serial numbers associated with the individual with the portable electronic devices 14 and in some cases, may also include serial numbers and corresponding programmable electronic keys 12. Individual users and/or programmable electronic keys 12 may then be assigned to correlate with a specified access transfer device 18 and/or authorized portable electronic device 14 (e.g., one user and/or portable electronic device 14 may be assigned serial numbers 1, 2, 3; while another user and/or portable electronic device 14 may be assigned serial numbers 1, 4, 5).

[0024] As noted earlier, in some embodiments, each programmable electronic key 12 may be authorized for specific locations, departments, and/or portable electronic devices 14. For instance, FIG. 5 shows that a manager may have authorization for all zones, locations, departments, and/or portable electronic devices 14 (indicated as numbers 1-6), while associate #1 may only have authorization for two zones, locations, departments, and/or portable electronic devices 14 (indicated as numbers 4 and 5), and associate #2 may only have authorization for one zone, location, department, or portable electronic devices 14 (indicated as number 6). As such, a retail store or other establishment may limit the scope of authorization for different associates within the same retail store. In order to accommodate different authorizations levels, each programmable electronic key 12 may be configured to store a code that is associated with each zone, location, department, and/or portable electronic devices 14. For example, each zone may include a plurality of portable electronic devices 14 and/or access transfer devices 18, and a retail store may have multiple zones (e.g., a zone for electronics, a zone for jewelry, etc.).

[0025] In some embodiments, each of the programmable electronic keys 12 may be programmed with the same security code using the programming station 16. In other embodiments, the setup process may be used in conjunction with a planogram of the access transfer devices 18 associated with the portable electronic devices 14. The planogram may represent a layout of a specified and/or desired location of each portable electronic device 14 within the retail store or other establishment. For example, at initial setup, the programmable electronic key 12 may be used to map serial numbers to specific portable electronic devices 14 on a planogram. As the programmable electronic key 12 communicates with the retail

merchandising system 26 the planogram containing the serial numbers of the portable electronic devices 14 is populated. This planogram may also be uploaded to a remote location or device such as a client-host network 32 for managing the planogram. As specified before, particular serial numbers may also be assigned to authorized users.

[0026] In one embodiment, as shown in FIG. 6, the access authorization system 10 is part of a client-host network 32 of access transfer devices 18 and portable electronic devices 14. The client-host network 32 may be cloud-based for receiving data from, and/or providing data to, the access transfer devices 18, programmable electronic keys 12 and/or retail merchandising system 26. According to some embodiments, the client-host network 32 enables communication between a plurality of access authorization systems 10. The client-host network 32 may facilitate data transfer to one or more remote portable electronic devices 14 and/or one or more remote locations where the data may be accessed, reviewed and analyzed. The client-host network 32 may be a mesh network (see FIG. 6) including a plurality of nodes 20 that are configured to communicate with one another, one or more programmable electronic keys 12 and/or one or more access transfer devices 18. The nodes 20 and/or access transfer devices 18 may be located within one or more zones defined in the store. A gateway 24 may be employed to allow for communication between the one or more nodes 20 and the cloud 22. In some embodiments, all communication within the client-host network 32 may be wireless, such as via radio-frequency signals (e.g., Sub GHz ISM band or 2.4 GHz), although other types of wireless communication may be possible.

[0027] Various techniques may be used to initially program the electronic keys 12 and the portable electronic devices 14. For example, the access transfer devices 18 may be initially connected to an authorized portable electronic device 14. Upon communication with the portable electronic device 14 or the client-host network 32, the access transfer device 12 and/or programmable electronic key 12 may provide data to the portable electronic device. For instance, the electronic key 12 may provide a security code to the portable electronic device 14 to be stored. A programming station 16 may provide a security code or other data to the portable electronic device 14, the access transfer device 18 and/or the programmable electronic key 12. In some instances, a client-host network 32 may communicate the security code or other data to

each of its authorized portable electronic devices 14. Each programmable electronic key 12 may only need to be programmed once. In some embodiments, a programming station 16 may be located within each zone, and a programmable electronic key 12 may receive a code from each programming station 16 to which it is authorized. Thereafter, each programmable electronic key 12 may need to be "refreshed" at the programming station 16 or a charging station 19 following a predetermined period of time. In other embodiments, the programmable electronic key 12 and/or the portable electronic device 14 may be programmed directly via the client-host network 32. In one embodiment, the portable electronic device 14 may be programmed without the programming station. For example, the portable electronic device 14 may include software for generating and/or storing security codes or other similar data.

[0028] In some embodiments, each programmable electronic key 12 may be configured to store various types of data. For example, the electronic key 12 may store a serial number of one or more portable electronic devices 14, the data and time of activation of the programmable electronic key 12, a user of the programmable electronic key 12, a serial number of the programmable electronic key 12, a department number within a retail store, number of individual programmable key 12 activations, a type of activation (e.g., "naked" activation, activation transferring only data, activation transferring power, activation transferring data and power), and/or various events (e.g., a merchandise security device has been locked, unlocked, armed, or disarmed). For instance, the identity of a user of a programmable electronic key 12 may be communicated to a remote location or retail merchandising system 26. This information may be transmitted to the remote location or retail merchandising system 26 upon each activation of the programmable electronic key 12 or at any other desired period of time, such as upon communication with a programming or authorization station 16. Thus, the data transfer may occur in real time or automatically in some embodiments. In some cases, the programming station 16 may be configured to store the data and transfer the data to a remote location or retail merchandising system 26. Authorized personnel may use this data to take various actions, such as to audit and monitor associate activity, determine the battery life of a programmable electronic key 12, audit the portable electronic devices 14, etc. Moreover, such information may be requested and obtained on demand, such as from the programming station 16 and/or through the

client-host network 32.

[0029] In other embodiments, data stored by the programmable electronic key 12 may include battery analytics of a programmable electronic key 12. For example, the battery analytics may include monitoring the battery voltage of a programmable electronic key 12 when the programmable electronic key 12 is placed on a charging station 18 and the time taken to reach full charge. These values may be used to determine depth of discharge. The battery analytics may be indicative of a battery that is nearing its end of life. A retailer or other authorized personnel may take various actions using this information, such as replacing and/or disabling the programmable electronic key to prevent battery swelling and housing failure.

[0030] In one embodiment, the access transfer device 18 and/or the programmable electronic key 12 may include a time-out function. More particularly, the ability of the access transfer device 18 and/or the programmable electronic key 12 to authorize access to and/or to transfer data and/or power to the portable electronic device 14 may be deactivated after a predetermined time period. For example, the access transfer device 18 and/or the programmable electronic key 12 may be deactivated after about six to about twenty-four hours from the time the programmable electronic key 12 was programmed or last refreshed. In this manner, an authorized employee/manager/sales associate typically must program or refresh their assigned programmable key 12 at the beginning of each work shift. In other embodiments, the charging station 18 may be configured to deactivate the access transfer device 18 and/or programmable electronic key 12 is positioned within or otherwise engaged with a charging port 30 (see, e.g., FIG. 1). In this manner, the charging station 18 can be made available to an authorized employee/manager/sales associate. In one embodiment, the programmable electronic key 12 may be authorized upon the sales associate inputting an authorized code to release the programmable electronic key 12 for use. For instance, the employee/manager/sales associate may input a code on a keypad 44 in communication with the charging station 18. Upon inputting the correct code, the charging station 18 may indicate which programmable electronic key 12 is authorized for use by the employee/manager/sales associate (e.g., via an audible and/or a visible indicator). In some embodiments, the time-out period may be predetermined or customized by a user. For example, a manager of a retail store may input a particular time period for one or more

of the access transfer devices 18 and/or programmable electronic keys 12. Those access transfer devices 18 and/or programmable electronic keys 12 that are "active" may be monitored via communication within the client-host network 32. In other embodiments, the access transfer device 18 and/or programmable electronic key 12 may be timed out or otherwise disabled in response to an event. For instance, the access transfer device 18 and/or programmable electronic key 12 may be disabled in response to the access transfer device 18 and/or programmable electronic key 12 being misplaced or stolen, or access transfer devices 18 and/or programmable electronic keys 12 being brought into a retail store that are not authorized for use with that particular store. Such disabling may occur via a command sent to the access transfer device 18 and/or programmable electronic the electronic key 12 via the client-host network 32 or retail merchandising system 26.

[0031] As noted above, in some embodiments, the authorization access system 10 may be configured to communicate with software or firmware installed by the retailer on a retail merchandising system 26 for obtaining and facilitating communication of data. The software may also allow for a retailer to remotely provide information to the portable electronic device 14, such as sending various updates, as well as interface with the portable electronic device 14. In one embodiment, commands may be provided remotely for taking various actions. For example, where a theft has occurred, a command may be provided from a remote location or retail merchandising system 26 (e.g., a tablet or computer) to lock and/or arm all or a portion of the access transfer devices 18 and/or portable electronic devices 14. Similarly, a command may be provided from a remote location or retail merchandising system 26 to deactivate all or a portion of the programmable electronic keys 12. As such, techniques may be provided for centralized security and control of the access transfer devices 18, programmable electronic keys 12, portable electronic devices 14, and other components within the retail merchandising system 26.

[0032] The foregoing has described one or more exemplary embodiments of a merchandise display security system. Embodiments of a merchandise display security system have been shown and described herein for purposes of illustrating and enabling one of ordinary skill in the art to make, use and practice the invention. Those of ordinary skill in the art, however, will readily understand and appreciate that numerous variations and modifications of the invention

may be made without departing from the spirit and scope thereof. Accordingly, all such variations and modifications are intended to be encompassed by the appended claims.

That which is claimed is:

1. An access authorization system comprising:

at least one portable electronic device;

at least one access transfer device configured to communicate with the at least one portable electronic device; and

at least one electronic key configured to communicate data to the portable electronic device,

wherein the at least one electronic key is configured to communicate with the at least one access transfer device to provide an authorized user access to the at least one portable electronic device based on the data communicated by the electronic key.

2. The access authorization system of Claim 1, wherein the at least one access transfer device comprises an adapter cord operably connected thereto, and wherein the adapter cord comprises a connector operably connected at a free end configured to releasably engage a corresponding port on the at least one portable electronic device.

3. The access authorization system of Claim 2, wherein the connector is a USB connector.

4. The access authorization system of Claim 1, wherein the access transfer device comprises an access transfer port for facilitating communication with the electronic key.

5. The access authorization system of Claim 4, wherein the at least one portable electronic device is configured to store at least one security code, and wherein the at least one electronic key is configured to store at least one security code.

6. The access authorization system of Claim 5, wherein the at least one electronic key is configured to communicate with at least one access transfer device to determine whether the security codes match, and wherein the at least one access transfer device is configured to authorize access to the at least one portable electronic device when the security codes match.

7. The access authorization system of Claim 5, wherein the at least one electronic key is configured to communicate with at least one access transfer device to determine whether the security codes match, and wherein the at least one access transfer device is configured to deny access to the at least one portable electronic device when the security codes do not match.

8. The access authorization system of Claim 1, wherein the at least one portable electronic device has a serial number, and wherein the at least one electronic key is configured to store the serial number.

9. The access authorization system of Claim 8, wherein the at least one electronic key is configured to communicate with the at least one access transfer device to determine whether the serial numbers match, and wherein the at least one access transfer device is configured to authorize access to the at least one portable electronic device when the serial numbers match.

10. The access authorization system of Claim 8, wherein the at least one electronic key is configured to communicate with the at least one access transfer device to determine whether the serial numbers match, and wherein the at least one access transfer device is configured to deny access to the at least one portable electronic device when the serial numbers do not match.

11. The access authorization system of Claim 1, wherein the data comprises a code and/or a serial number.

12. A method for authorizing access to a portable electronic device, the method comprising:

providing at least one portable electronic device;

providing at least one access transfer device configured to communicate with the at least one portable electronic device;

providing at least one electronic key configured to communicate with the at least one

access transfer device; and

initiating communication between the at least one electronic key and the at least one access transfer device for authorizing access to the at least one portable device based on data communicated by the electronic key.

13. The method of Claim 12, further comprising programming the at least one electronic key and the portable electronic device with the data.

14. The method of Claim 13, further comprising initiating communication between the at least one electronic key and the at least one access transfer device for authorizing access to the at least one portable device in response to the data programmed in the electronic key matching the data programmed in the corresponding portable electronic device.

15. The method of Claim 14, further comprising providing the access transfer device with an adaptor cord having a connector at a free end thereof.

16. The method of Claim 15, further comprising releasably engaging the connector with a corresponding port on the at least one portable electronic device such that the access transfer device is operably connected with the at least one portable electronic device.

17. The method of claim 16, wherein releasably connecting comprises releasably connecting a USB connector to the portable electronic device.

18. The method of Claim 12, further comprising providing the electronic key with one or more security codes and/or one or more serial numbers associated with the portable electronic device for authorizing access.

19. The method of Claim 18, further comprising initiating communication between the electronic key and the access transfer device to determine whether the security codes and/or one

or more serial numbers match, wherein the access transfer device is configured to authorize access to the portable electronic device when the security codes and/or serial numbers match.

20. An access authorization system comprising:

at least one portable electronic device having data associated therewith;

at least one access transfer device configured to communicate with the at least one portable electronic device; and

at least one electronic key configured to store data,

wherein the at least one electronic key is configured to communicate with the at least one access transfer device for authorizing access to the at least one portable electronic device in response to the data stored in the at least one electronic key matching the data associated with the at least one portable electronic device.

21. The access authorization system of Claim 20, further comprising a plurality of portable electronic devices, a plurality of access transfer devices, and a plurality of electronic keys; wherein each one of the plurality of electronic keys is configured to communicate with a respective one of the plurality of access transfer devices for authorizing access to one of the plurality of portable electronic devices in response to the data stored by the respective electronic key matching the data associated with the respective portable electronic device.

22. The access authorization system of Claim 20, wherein the at least one electronic key is configured to store a security code and/or a serial number associated with one or more portable electronic devices for authorizing access to the one or more portable electronic devices.

ABSTRACT

An access authorization system including an electronic portable device, an access transfer device and an electronic key. The access transfer device is configured to be operably connected to the portable electronic device and the electronic key is configured to communicate with the access transfer device to authorize and/or deny user access to the portable electronic device.

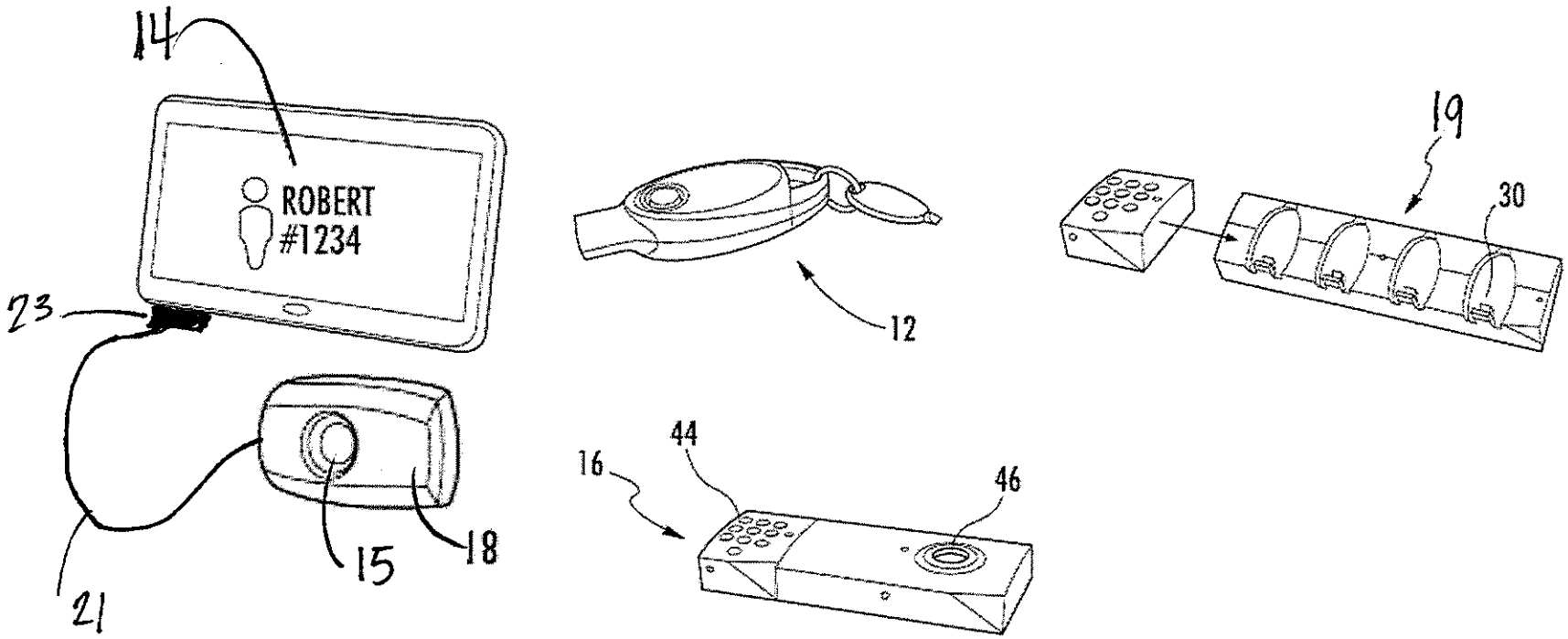

FIG. 1

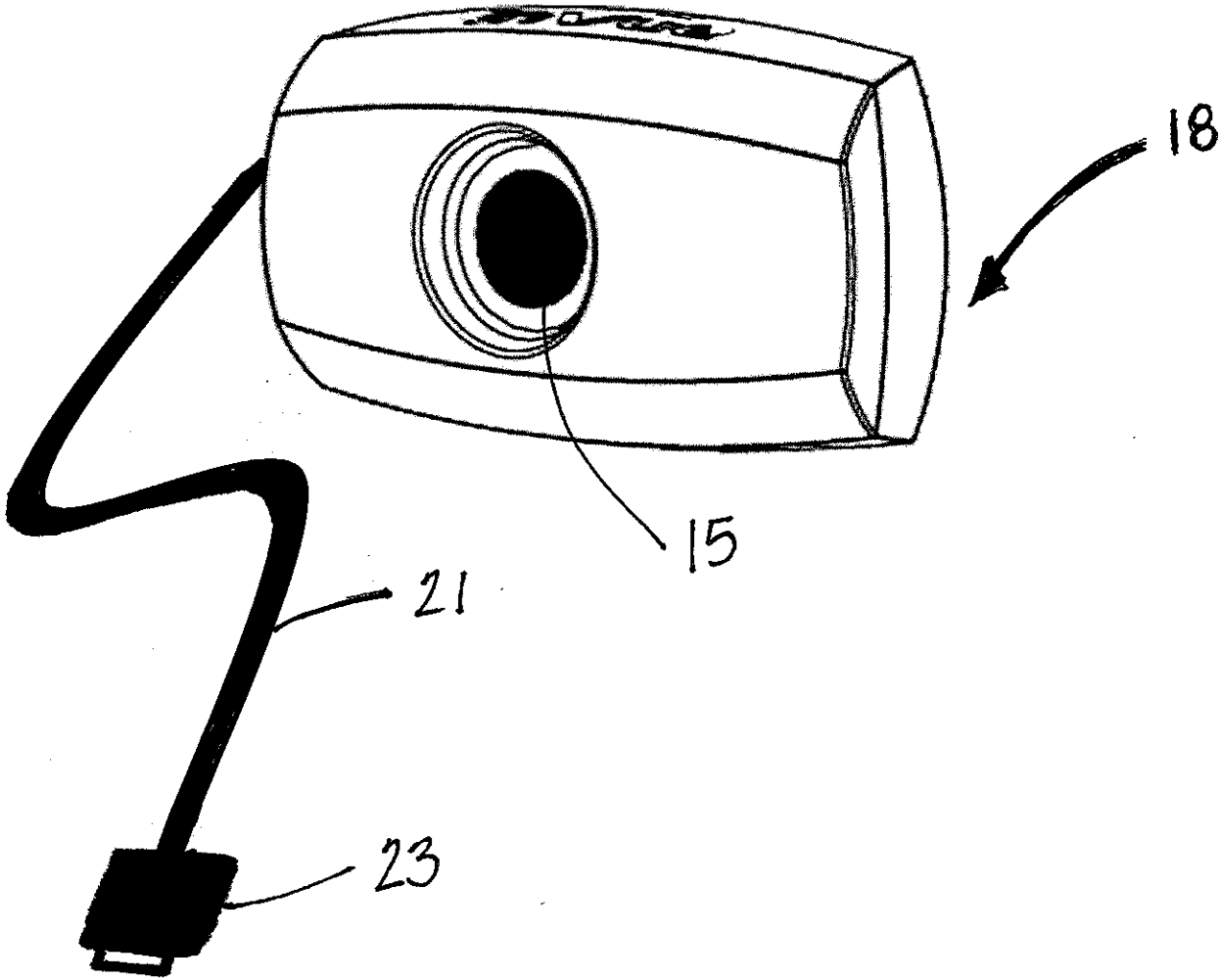

FIG. 2

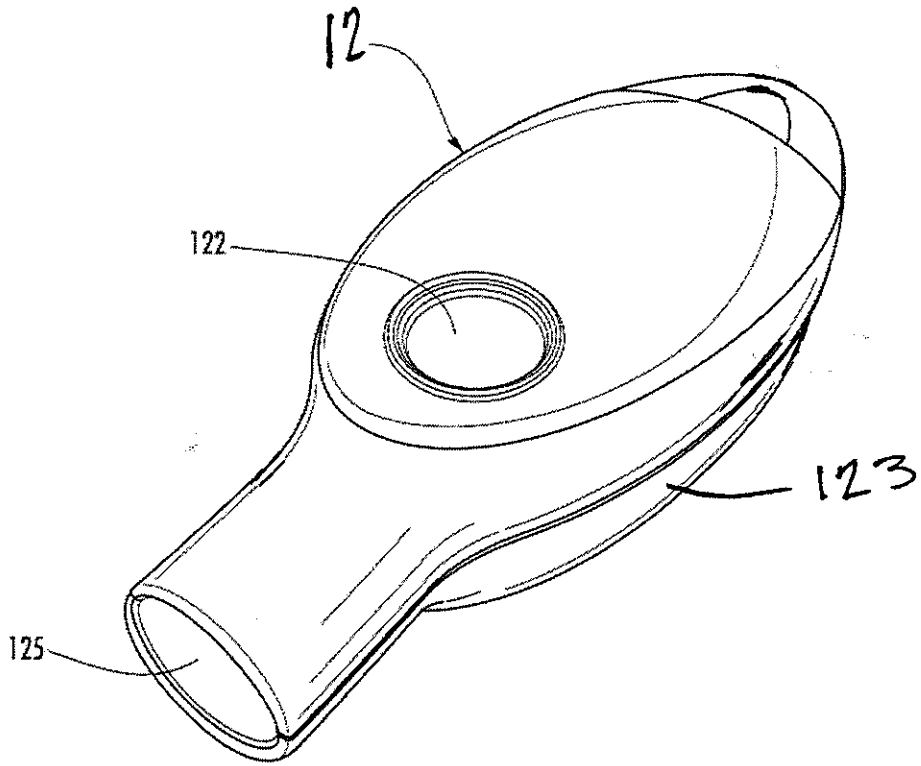

FIG. 3

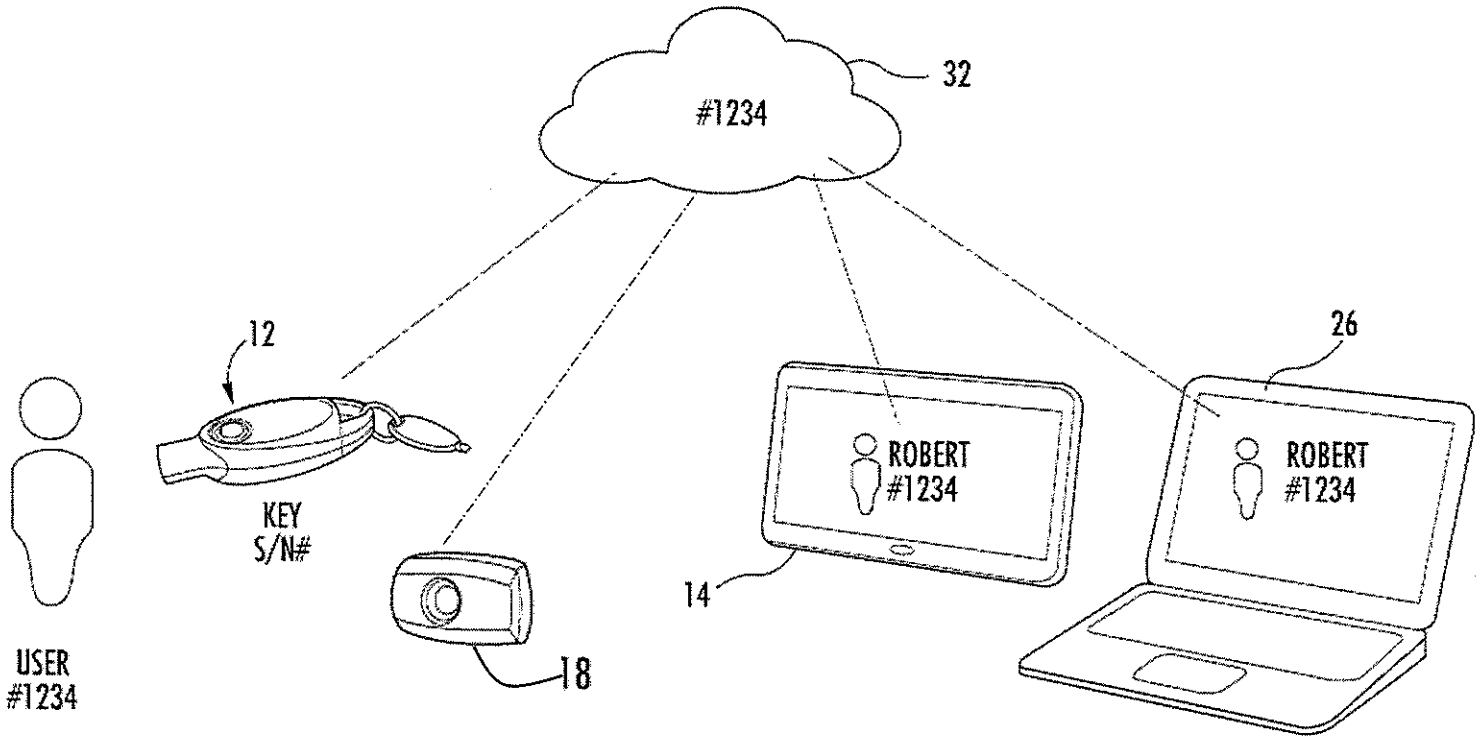

FIG. 4

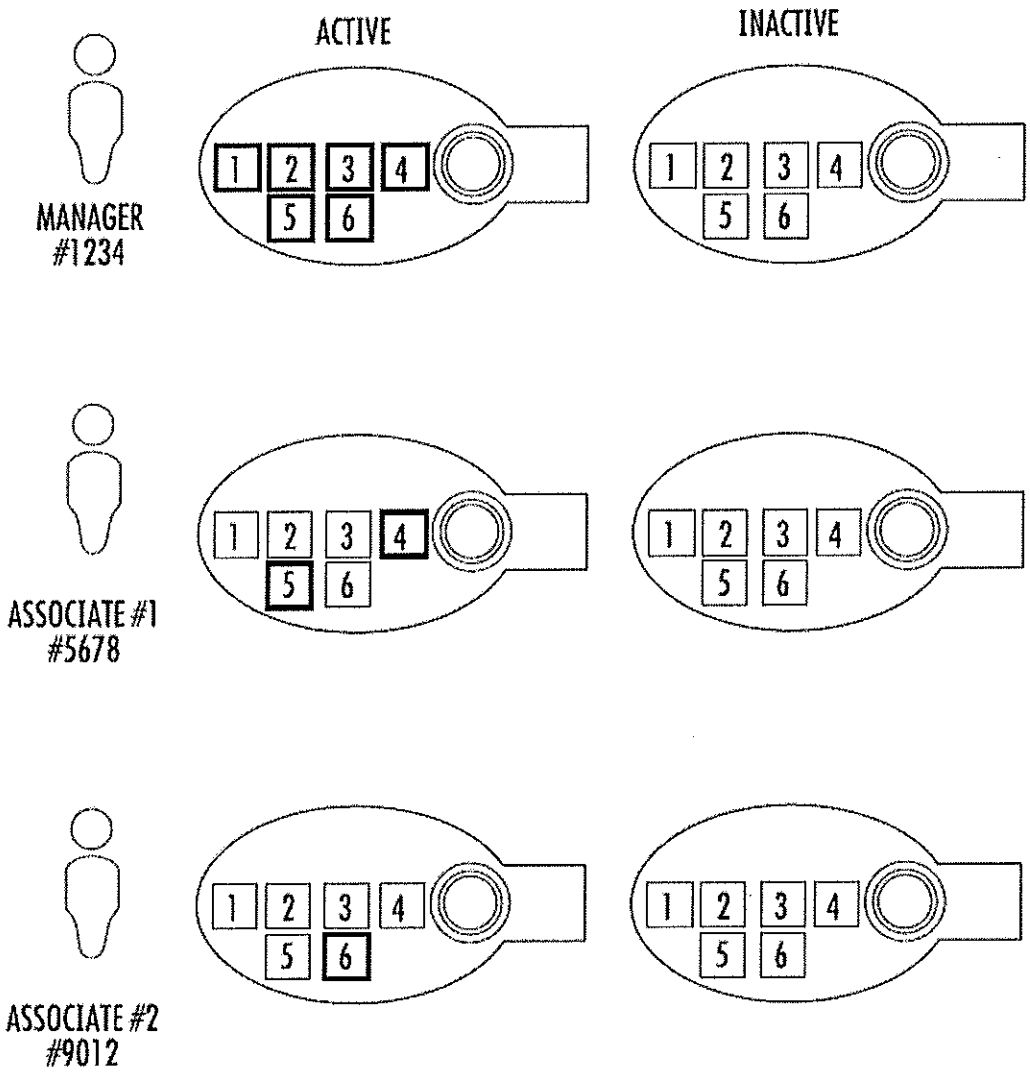
ACTIVE
INACTIVE
MANAGER
#1234
ASSOCIATE #1
#5678
ASSOCIATE #2
#9012
1
2
3
4
5
6

FIG. 5

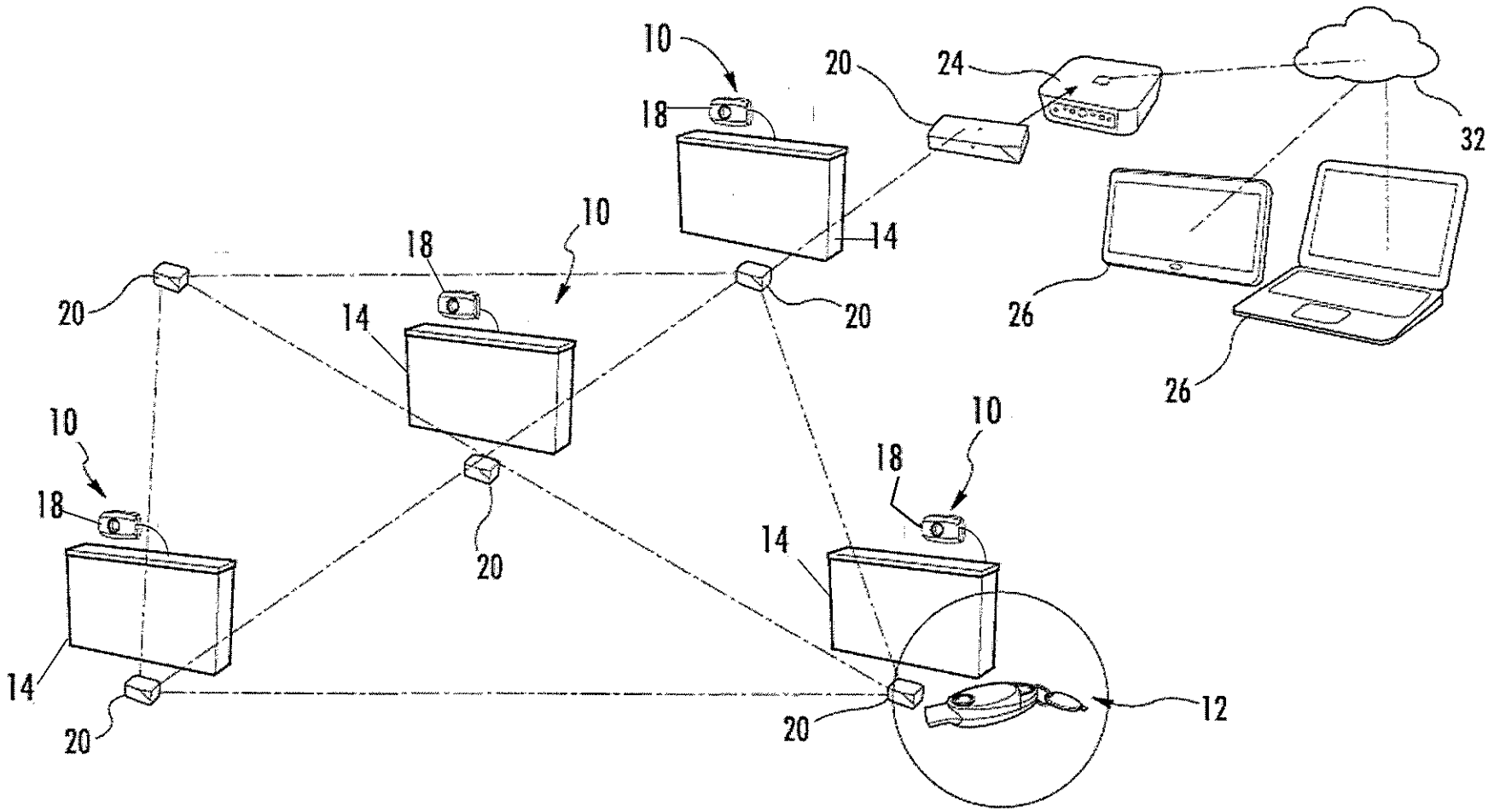

FIG. 6