



(51) International Patent Classification:

G06F 1/00 (2006.01) G06F 21/30 (2013.01)  
G06F 13/14 (2006.01) G06F 21/60 (2013.01)

(21) International Application Number:

PCT/US2013/026517

(22) International Filing Date:

15 February 2013 (15.02.2013)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/599,815 16 February 2012 (16.02.2012) US  
61/600,546 17 February 2012 (17.02.2012) US

(71) Applicant: MASTER LOCK COMPANY [US/US]; 137  
W. Forest Hill Avenue, Oak Creek, Wisconsin 53154 (US).

(72) Inventors; and

(71) Applicants : BARTUCCI, John [US/US]; 80 Talsmon  
Dr., Crystal Lake, IL 60012 (US). HEPPNER, John

[US/US]; 932 E. Kilbourn Ave. #1902, Milwaukee, WI  
53202 (US). TRAPANI, Matt [US/US]; 931 Oxford Rd.,  
Deerfield, IL 60015 (US). ZHANG, Yi [US/US]; 732 E.  
Village Green Ct., Oak Creek, WI 53154 (US).

(74) Agents: REICHENBERGER, Karl, F. et al.; Foley &  
Lardner LLP, 3000 K. Street N.W., Washington, District of  
Columbia 20007-5109 (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, CZ, DE, DK, DM,  
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,  
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,  
KR, KZ, LA, LC, LR, LS, LT, LU, LY, MA, MD, ME,  
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,  
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,  
RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ,  
TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,  
ZM, ZW.

[Continued on next page]

(54) Title: DATA STORAGE DEVICES, SYSTEMS, AND METHODS

(57) Abstract: A portable electronic memory device (e.g., USB flash  
drive) is shown and described. Embodiments include portable electron-  
ic memory devices having a keypad, encryption hardware, and the abil-  
ity to encrypt, decrypt, or serve as an authentication tool for a remote  
computing system without requiring special drivers to be installed on  
the receiving system.

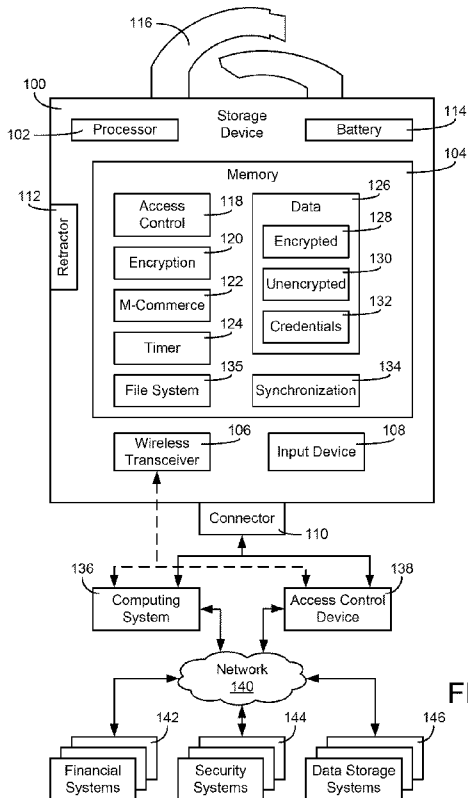


FIG. 1



**(84) Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

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

## DATA STORAGE DEVICES, SYSTEMS, AND METHODS

### CROSS-REFERENCE TO RELATED APPLICATIONS

**[0001]** This application claims the benefit of and priority to 61/599,815, filed Feb. 16, 2012 and 61/600,546, filed Feb. 17, 2012, the entireties of which are incorporated herein by reference.

### BACKGROUND

**[0002]** The present disclosure relates generally to the fields of data security and access control systems. The disclosure relates more specifically to portable devices configured to securely store data and/or control access to secure resources.

**[0003]** Portable storage devices, such as Universal Serial Bus (USB) flash drives, allow users to carry data with them in a convenient manner and access the data on any compatible device to which the storage devices can be connected. Flash drives are often designed to have small enclosures so that the drives can be easily carried by a user in a pocket or on a keychain. For example, a user can load data from a workplace computer onto a flash drive, carry the flash drive to his residence, and transfer the data onto a home computer. Other than transferring and/or storing data from computing devices, many portable storage devices are limited in their functionality. Further, many portable storage devices have limited security features.

### SUMMARY

**[0004]** A portable electronic memory device (e.g., USB flash drive) is shown and described. Embodiments include portable electronic memory devices having a keypad, encryption hardware, and the ability to encrypt, decrypt, or serve as an authentication tool for a remote computing system without requiring special drivers to be installed on the receiving system.

**[0005]** According to one embodiment of the invention, a portable electronic memory device includes a housing and a non-transient computer-readable media within the housing. The device further includes a plurality of key buttons disposed upon the housing and configured to allow entry of a security code by a plurality of

keystrokes. The device further includes a communications interface for communication with external electronics that are not a part of the portable electronic memory device. The device yet further includes a circuit which has a locked state and an unlocked state. The correct entry of the security code is required to enter the unlocked state. The unlocked state permits access to first data of the non-transient computer-readable media which is inaccessible in the locked state. The entry of the security code also causes second data comprising a key to be generated and made available to the external electronics via the communications interface. The communications interface may be a universal serial bus (USB) interface.

**[0006]** In some embodiments the device further includes a padlock shackle extending from the housing and wherein the housing comprises a blocker solenoid for locking or unlocking the padlock shackle. The circuit may encrypts the first data and the key for transmission via the communications interface. The circuit may associate different keypad combinations with a different activities.

**[0007]** A first keypad combination is used to transition the device between the locked state and the unlocked state. A second keypad combination generates authenticating data for at least one of: (a) a physical device entry code, (b) a commercial transaction, (c) authentication with a remote server. The circuit may be configured to associate different keypad combinations with different pieces of data to be selectively secured and made available for transmission via the communications interface. Making the data including the key available to the external electronics may include permitting the key to be forwarded as a text string. Making the data including the key available to the external electronics may also or alternatively include generating a file containing the key in the non-transient computer-readable media and permitting the key to be uploaded to a remote server via the electronics.

**[0008]** The circuit may be configured to transmit the data comprising the key to the external electronics via the communications interface in response to input received from the plurality of key buttons.

**[0009]** The circuit may include a timer and wherein the timer may delete the data after a period of time counted using the timer. The circuit may include an evaluation module and a timer and wherein the evaluation module deletes the key if a valid request for the key is not received with a period of time counted using the

timer. The circuit encrypts the first data stored on the memory device using the key generated by entry of the security code. The circuit receives a second key via the communications interface and encrypts the key generated by entry of the security code using the second key. The circuit makes the encrypted first data and the encrypted key available for transmission via the communications interface.

**[0010]** The communications interface may be an active or passive RFID interface. The generated key may be made available for reading or writing via the RFID interface. The circuit may maintain a history of unlock, lock, and/or transfer events in the non-transient computer readable media. The circuit may control a solenoid to allow or prevent the communications interface from being extended outside of the housing. The circuit may include a tamper detection module configured to determine whether the housing has been compromised and to cause the first data to be destroyed in response to a determination that the housing has been compromised. The data may also or alternatively be destroyed in response to a panic button being pressed or another condition being detected. The device may further include an electronic display coupled to the housing. The circuit may control the display to cause at least one of a tamper alert and a keypad entry status to be indicated via a state change of the display. In an exemplary embodiment the housing is precisely filled with epoxy to make the USB device relatively water-proof, crush-proof, and/or fire-proof. Other methods of fire-proofing, water-proofing, and/or crush-proofing may be provided.

**[0011]** Another embodiment relates to a method for controlling access to a remote server using a portable electronic memory device. The method includes receiving an access request at a portable electronic device from the remote server. The method further includes receiving user input via a keypad on the portable electronic device. The method also includes checking the keypad entry on the portable electronic device and providing an authentication response to the remote server if the keypad entry is verified. The method further includes providing access to the remote server from a third device associated with the user. The third device may be a local computing device in communication with the portable electronic device locally and in communication with the remote server via a wide area connection. The portable electronic memory device may be a USB dongle having the keypad and memory local to the USB dongle. The access controlled may be

virtual private network access between the local computing device and the remote server.

**[0012]** Another embodiment relates to a method for controlling access to first data on a portable electronic memory device. The method includes temporarily generating and exposing second data for providing to a remote authenticator in response to entry of a correct user input sequence at a user input device. The method further includes, at the remote authenticator, granting user permissions to the first data in response to a determination that the second data is authentic. The remote authenticator may use a key stored at the mobile authenticator and associated with the portable electronic device to decrypt the second data received from the portable electronic device. The method may further include checking the contents of the decrypted data to determine whether or not the second data is authentic.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0013]** FIG. 1 is a block diagram of a storage device according to an exemplary embodiment.

**[0014]** FIG. 2 is a block diagram of a storage device according to another exemplary embodiment.

**[0015]** FIG. 3 is a flow diagram of a process for enabling access to secure data stored on a storage device according to an exemplary embodiment.

**[0016]** FIG. 4 is a flow diagram of a process for enabling wireless access to secure data stored on a storage device according to an exemplary embodiment.

**[0017]** FIG. 5 is a flow diagram of a process for enabling access to a resource secured by an access control device using a storage device according to an exemplary embodiment.

**[0018]** FIG. 6 is a flow diagram of a process for authorizing a transaction using a storage device according to an exemplary embodiment.

**[0019]** FIGS. 7A through 13D are illustrations of storage devices according to various exemplary embodiments.

## DETAILED DESCRIPTION

**[0020]** Before turning to the figures, which illustrate the exemplary embodiments in detail, it should be understood that the application is not limited to the details or methodology set forth in the description or illustrated in the figures. It should also be understood that the terminology is for the purpose of description only and should not be regarded as limiting.

**[0021]** A portable electronic memory device (e.g., USB flash drive) is shown and described. Embodiments include portable electronic memory devices having a keypad, encryption hardware, and the ability to encrypt, decrypt, or serve as an authentication tool for a remote computing system without requiring special drivers to be installed on the receiving system.

**[0022]** Referring generally to the figures, apparatus, systems, and methods for storing and/or utilizing secure data and/or for controlling access to secure resources are provided according to various exemplary embodiments. Electronic data has grown increasingly sensitive (e.g., personal and/or corporate data) as more types of data have begun to be stored and transferred in electronic form. The sensitivity of data raises concerns about what might be done with the data if it were to become available to unauthorized persons (e.g., if a USB flash drive were misplaced or stolen). Some portable storage devices address this concern by enabling users to encrypt data on the drive using hardware or software-based data encryption methods. Most portable storage devices are passive storage devices that have functionality that is limited to storing and transferring data under control of software (e.g., encryption software) that must be installed on the

**[0023]** Various exemplary embodiments described in the present disclosure provide features relating to securing and utilizing data and/or controlling access to resources with and/or within the convenience of a portable storage device. Some exemplary storage devices may be configured to store various types of information, at least some of which may be secure or encrypted, and allow a user to access secure information by providing an access key (e.g., a key combination or other input) using an input device (e.g., keypad) of the storage device. Some information may be encrypted, such that only an individual having the appropriate access key may access the information, while other information may be left unsecured, such

that any individual with access to the storage device can access the unsecured data.

**[0024]** In some embodiments, different levels of security may be implemented. For example, a storage device may be configured to store multiple access keys that unlock access to different resources stored on the storage device, so that a user with a first access key can access a first set of information and a user with a second access key can access a different second set of information. In some embodiments, the storage device may be configured to allow a user to back up data stored on the storage device to a remote storage device or data storage service. In some embodiments, the storage device may be configured to delete or destroy some or all of the stored data after a predetermined number of consecutive failed attempts to enter an access key (e.g., in order to prevent the data from being accessed by unauthorized parties). Various embodiments enable end-to-end data security (e.g., internet security, data synchronization, commerce transactions, etc.) using the data storage device.

**[0025]** In some exemplary embodiments, the data storage device may include a wireless capability, such as radio frequency identification (RFID) (e.g., reading and/or writing), for use in transmission of data to other devices and/or controlling access to secured resources (e.g., data or physical resources). A wireless communication device such as a RFID transceiver or tag may be used for different functions according to various embodiments of a data storage device. For example, financial data or rewards account data may be wirelessly transmitted from the data storage device to a payment processing system, such as a point-of-sale payment device, upon user entry of a payment key code on the storage device. In another exemplary embodiment, the wireless communication device may be used to control access to secured resources, such as a car, house, safe, etc., by placing the storage device in proximity to an access control device of the secured resource and entering an access key code on the storage device. In other examples, the wireless communication device may allow a computer to wirelessly access data stored on the data storage device, wirelessly obtain credentials needed to access data stored on a remote storage device, and/or synchronize data stored on the storage device with a remote storage device.

**[0026]** Referring now to FIG. 1, a block diagram of a storage device 100 is shown according to an exemplary embodiment. Device 100 may be configured to perform

some or all of a variety of different functions according to various exemplary embodiments. In some embodiments, device 100 may be configured to enable a user to securely access data stored on device 100, such as sensitive data, authentication credentials, financial information, etc. by requiring entry of an access key code on device 100. In some embodiments, device 100 may be configured to enable fast, easy, and secure financial transactions using credential and/or financial information stored on device 100. In some embodiments, device 100 may be configured to control access to resources or physical locations, such as by unlocking doors having an electronic access control device.

**[0027]** Storage device 100 includes a processor 102 that is configured to execute instructions to implement the various functions of device 100. Processor 102 may be any general purpose or special purpose processor (e.g., FPGA, CPLD, ASIC, etc.). Instructions and/or data may be stored on a memory 104 of device 100, which may be any type of computer-readable medium (e.g., RAM, ROM, EPROM, EEPROM, hard drive, flash memory, etc.). In some embodiments, memory 104 may include flash memory. The use of flash memory may help device 100 to have a small form factor, such that device 100 may be highly portable and easily carried in a pocket, clipped to a bag, connected to a set of keys and/or used as a key fob. In some embodiments, device 100 may include a clip, shackle, or other type of coupling device 116 configured to allow device 100 to be coupled to another object, such as a keychain or a bag.

**[0028]** Device 100 includes an input device 108 configured to receive user input that may be used to unlock certain data and/or functions of device 100. In some embodiments, input device 108 may include a keypad configured to receive one or more user key codes, such as a combination of numbers, letters, and/or symbols. In some embodiments, the key code may include a personal identification number (PIN), which may be a sequence of numbers (e.g., four, six, eight, nine, ten, etc.). In various embodiments, the key code may be predetermined for each storage device or may be determined by a user. In some embodiments, input device 108 may support keypad randomization (e.g., may include a software-based keypad configured to reorganize the order/placement of keys) to mitigate the risk of fingerprint lifting being used to deduce a key code. In some embodiments, input device 108 may include a device other than or in addition to a keypad, such as a dial, a biometric scanner (e.g., a fingerprint scanner), or another input device.

**[0029]** Device 100 may include a connector 110 configured to operably (e.g., communicatively and/or electrically) connect device 100 to another device, such as a computing device (e.g., laptop, desktop, tablet, smartphone, portable entertainment device, etc.). In one embodiment, connector 110 may be or include a male Universal Serial Bus (USB) connector configured to mate to a female USB connector (e.g., of a computing device). In some embodiments, connector 110 may be or include various other types of connectors, such as mini-USB, micro-USB, Firewire, Thunderbolt, external Serial Advanced Technology Attachment (eSATA), proprietary connectors associated with various electronic devices, etc. In some embodiments, connector 110 may include multiple connectors (e.g., USB and mini-USB). In some embodiments, connector 110 may be configured to be coupled to attachments to convert connector 110 into a different format (e.g., a USB-to-mini-USB adapter). In some embodiments, connector 110 may be configured to transmit electrical power, such that device 100 may receive power from and/or provide power to a connected device. In some embodiments, device 100 may include a retractor 112 configured to retract connector 110 back within a main housing of device 100 to protect connector 110 from damage when not in use. Computing devices to which device 100 may be connected may include any of a variety of different operating systems, such as Microsoft Windows, Mac OS, Linux, Apple iOS, or Google Android.

**[0030]** In some exemplary embodiments, device 100 may include a wireless transceiver 106 configured to enable device 100 to communicate wirelessly with other devices, such as computing devices, access control devices, and/or payment processing devices. Wireless transceiver 106 may be configured to transmit and/or receive signals from various types of electronic devices using various types of communication methods. In some embodiments, wireless transceiver 106 may include a RFID transceiver configured to enable device 100 to communicate with (e.g., read from, write to) other RFID devices. The RFID transceiver may include a powered or active RFID transceiver or a passive RFID tag powered wirelessly by devices with which the RFID tag communicates (e.g., external RFID readers or writers). One or more types of close proximity communication may be enabled using wireless transceiver 106, such as various forms of RFID (e.g., near field communication (NFC)), MIFARE, HID-based proximity communication, etc.). According to an exemplary embodiment, the device 100 is configured to receive

content by reading a separate RFID tag (or other type of near field communication device) brought within proximity of the wireless transceiver 106. Upon reading and receiving the content, the device 100 may automatically cause the content to be recorded by a connected computer and/or provided to a remote server. In other words, in some embodiments, the device 100 may serve as a bridge between RFID-read content and computing resources such as a local computer or a remote server. The keypad may be used to initiate or authenticate a transaction, or to put the device 100 in a state for reading and receiving the RFID information.

**[0031]** In some embodiments, wireless transceiver 106 may be configured to communicate wirelessly with other devices (e.g., computing devices) using one or more wireless communication protocols or methods such as RFID, Bluetooth, Wi-Fi, radio frequency (RF) communication, infrared (IR) communication, and/or any other type of wireless communication. In some embodiments, wireless transceiver 106 may include multiple different types of wireless transceivers and/or may be configured to enable wireless communication under multiple different methods of wireless communication (e.g., RFID, Bluetooth, and Wi-Fi).

**[0032]** In some embodiments, device 100 may include a battery 114 (e.g., rechargeable battery) configured to power various components of device 100 (e.g., when not connected to an external power source, such as through connector 110). For example, battery 114 may be configured to provide power to processor 102, wireless transceiver 106, input device 108 (e.g., an electronic keypad), and/or other various components of device 100. In some embodiments, battery 114 may be configured to be charged through connector 110 (e.g., trickle-charged through a USB port of a computer, charged more quickly through connection to a USB-configured wall adapter, etc.).

**[0033]** Memory 104 may include various computer code modules for execution by processor 102 to implement various functions of device 100. Memory 104 may include an encryption module 120 configured to encrypt data stored on and/or transferred to or from device 100. Encryption module 120 may be configured to encrypt data using any encryption standard, such as FIPS standards (e.g., DES, triple DES, etc.), AES, or another type of encryption. In some embodiments, device 100 may be HIPAA, SOX, and/or GLB compliant. In some embodiments, an encryption algorithm or scheme utilized by encryption module 120 may be or include a FIPS 140-1, FIPS 140-2, FIPS 140-3, and/or FIPS 140-4 compliant

encryption algorithm or scheme. In some embodiments, device 100 may utilize an ANSI X9.31 random number generator as part of an encryption process. Memory 104 may be configured to store the encrypted data 128. In some embodiments, data 126 may additionally or alternatively include unencrypted data 130 that has not been encrypted by encryption module 120. In some embodiments, data 126 may additionally or alternatively include credential data 132 that may include credentials used to authenticate a user and/or a user account for various applications (e.g., secure websites, financial services, access control devices, etc.). Data 126 may include any type of data a user wishes to store on device 100, such as miscellaneous computer files, medical/healthcare data, travel documents such as passports, confidential information such as a social security number, and/or other types of data. Information that is confidential, sensitive, and/or that the user may wish to prevent from being accessed by unauthorized persons may be encrypted by encryption module 120 to prevent the data from being accessed in the event device 100 is lost or stolen.

**[0034]** In some embodiments, a user may access encrypted data 128 by providing a key code or other user input via input device 108. Once the key code has been entered, encryption module 120 may be configured to decrypt one or more portions of encrypted data 128 and allow a connected device (e.g., connected via connector 110 and/or wireless transceiver 106) to access the decrypted data. In some embodiments, different key codes may be configured to decrypt and/or provide access to different data stored on device 100. For example, a first key code may provide access to certain encrypted files but not medical data and passport-related files. A second key code may provide access to all encrypted data. In this manner, a user may control which users have access to certain secure data (e.g., by giving another user the first key code but not the second key code). In some embodiments, a user may be enabled to create or activate one or more guest key codes configured to allow guest access to certain secure resources but not others. For example, in some embodiments, access to all files on device 100 may be restricted until a first key code is entered (e.g., by not allowing connector 110 to be extended until the first key code is entered, by making file system 135 inaccessible to a connected device until the first key code is entered, etc.) and access to certain resources may be restricted until a second key code is entered, even if the first key code has been entered. In some embodiments, users may be

provided with a user interface on a computing device (e.g., a computing device to which device 100 is connected, an interface provided via a remote computer system such as a server and accessible to the computing device via a network, etc.) that may be used to set various customized parameters of device 100, such as the one or more access key codes.

**[0035]** In various embodiments, device 100 may utilize software and/or hardware encryption to encrypt data stored on device 100. Software encryption allows data to be encrypted without requiring a separate hardware circuit dedicated to encrypting data. Hardware encryption may allow files to be encrypted more quickly than software encryption and may improve the security of the data. The file system 135 of device 100, which organizes the storing of data in memory 104, may not be given access to the encryption key code that the user may enter into input device 108 to decrypt and access encrypted data 128 and/or credentials 132 (e.g., device 100 may support on-chip password matching).

**[0036]** In some embodiments, device 100 may be equipped with a timer 124 (e.g., a software module or hardware-based timer circuit) configured to restrict an idle time of device 100 before a user is required to re-authenticate with device 100 (e.g., by re-entering the user's key code). Timer 124 may be configured to monitor an amount of time that has elapsed since a last activity took place. Once a user enters a valid key code, timer 124 may start an idle timer. The idle timer may be restarted anytime the user performs certain activities pertaining to device 100, such as saving data to device 100, accessing data on device 100, using device 100 to access a resource that is secured by an access control device, performing a commerce transaction, or other activities. If the idle timer exceeds a threshold amount of time before another activity is performed, device 100 may require the user to re-authenticate in order to perform further actions. In some embodiments, the threshold amount of time, activities that trigger a reset of the idle timer, activities that may be performed if the idle timer exceeds the threshold, or other related variables may be configurable by the user. Timer 124 may help prevent unauthorized data access or use of device 100 in the event device 100 is left unattended, lost, forgotten, left plugged into a work device overnight, etc. In some embodiments, file system 135 may be configured to lock access to some or all of data 126 by a device to which device 100 is connected (until the user re-authenticates) once the idle timer exceeds the threshold.

**[0037]** In some embodiments, file system 135 may be configured to destroy part or all of data 126 after a threshold amount of consecutive failed/unauthorized access key code attempts. In some embodiments, the data may be destroyed by overwriting the data using specific patterns, multiple passes, etc. configured to prevent recovery of the original data after destruction. In various embodiments, most or all of the contents of memory 104, all of data 126, only encrypted data 128 and/or credential data 132, etc. may be destroyed. In some embodiments, a user may be enabled to select what types of data, if any, stored on device 100 are destroyed under a destruction procedure, how many consecutive failed attempts trigger destruction, a timeframe in which the attempts must be made to trigger destruction, and/or other aspects of the destruction procedure. In some embodiments, device 100 may be equipped with one or more sensors (e.g., contact sensors on a housing of device 100) configured to detect if device 100 is being tampered with, and device 100 may be configured to perform the destruction procedure if tampering is detected. The destruction procedure may help protect sensitive data stored on device 100 in the event device 100 is obtained by an unauthorized person who attempts to access the data (e.g., by guessing/hacking an access key code or by accessing memory 104 through brute force).

**[0038]** In some embodiments, device 100 may include a write protect switch. If the write protect switch is enabled, file system 135 may allow read-only access to files and may disallow any data to be written or modified on device 100.

**[0039]** A synchronization module 134 may be configured to enable device 100 to synchronize part or all of data 126 with a remote (e.g., network-based, cloud-based, Internet-accessible, etc.) data storage system 146 (e.g., Master Lock Vault). In some embodiments, the synchronization may occur manually through user access to a synchronization application stored on device 100, a connected device (e.g., computing system 136), or a network-enabled application stored on data storage system 146 or another remote system. Device 100 and/or computing system 136 may communicate with data storage system 146 through a network 140 (e.g., any wired or wireless communications network, such as using Ethernet, Wi-Fi, cable, satellite, or other transmission methods). In some embodiments, the synchronization may occur automatically upon connection of device 100 with certain other systems (e.g., upon user entry of a synchronization key code on input device 108 when connected with another device). The user may be enabled to

customize synchronization settings to specify what data is synchronized (e.g., all of data 126, just encrypted data 128, etc.), how often synchronization occurs, whether synchronization is performed manually, automatically, or both, and/or other aspects of synchronization. Once data has been synchronized, the data may be accessed by the user (e.g., through an authentication procedure with proper credentials, such as a username and password) on a computing device (e.g., connected or disconnected from device 100). In some embodiments, the credentials for accessing the interface of the remote data storage system may be stored on device 100, and the user may authenticate with data storage system 146 by entering a synchronization key code on user interface 108, which may transmit the credentials stored on device 100 to the computing device and, subsequently, to the authentication system for data storage system 146. In the event some or all of data 126 is destroyed (e.g., through damage to device 100 or through execution of a data self-destruction procedure), data may be recovered by device 100 or an authorized replacement by synchronizing with data storage system 146. In some embodiments, device 100 may be configured to synchronize with multiple data storage systems (e.g., for redundancy). In some embodiments, synchronization module 134 may be configured to transmit some or all of data 126 to other devices (e.g., other computing devices associated with the user, as specified by the user) as part of the synchronization procedure. In some embodiments, synchronization module 134 may be configured to synchronize some or all of data 126 with cloud-based storage systems.

**[0040]** In some embodiments, an application or interface provided by and/or executed on data storage system 146, a computing device operably connected to device 100, or on device 100 itself may be used to manage various settings and/or data stored on device 100. For example, the application/interface may be used to check memory usage on device 100, view types of information currently stored on device 100, input data to be stored on device 100 after a synchronization procedure is performed (e.g., credit card information), change settings associated with device 100 and/or data storage system 146, and/or perform other types of tasks relating to device 100. In some embodiments, settings that may be configurable may include, but are not limited to, an idle timeout, passwords and/or key codes, lighting and/or status identifier settings, a number of failed key code attempts that may be entered before data is destroyed, and/or other settings. In some embodiments, the

application/interface may be provided from data storage system 146 and/or another remote server and may be accessible on a computing device (e.g., a computing device connected to device 100) via a browser application executed on the computing device.

**[0041]** In some embodiments, the application or interface may be used to securely manage information stored on device 100. For example, the application/interface may enable a user to input financial or payment information (e.g., credit, debit, prepaid, and/or coupon information) and synchronize the data with device 100 through a secure, encrypted communication channel, such that the information is stored locally on device 100 after synchronization. In another exemplary embodiment, the application/interface may enable a user to enter authentication information for one or more access control devices that the user wishes to be able to access using device 100, and the authentication information may be securely transferred to device 100 upon synchronization. In some embodiments, the application/interface may communicate with one or more third party information services associated with the access control devices to obtain information needed to enable device 100 to successfully authenticate with the access control devices (e.g., communication protocols and/or data formats).

**[0042]** In some embodiments, a m-commerce module 122 may be configured to enable a user to perform mobile commerce, or m-commerce, and/or other types of transactions (e.g., financial transactions) using data stored on device 100. For example, the data may include financial data such as account information and/or credentials relating to a credit account, debit account, bank account, and/or prepaid account of the user. In some examples, the data may include a credit card, bank account, or debit account number, a debit PIN, a username, password, and/or other authentication information needed to authenticate with a network-enabled interface of one or more financial systems 142 associated with financial services. The data may be encrypted by encryption module 120 and stored as part of encrypted data 128 and/or credential data 132. Device 100 may be connected (e.g., through connector 110 and/or wireless transceiver 106) to a payment processing system configured to process the transaction. The connection may be direct or through an intermediary computing device (e.g., computing system 136). A request for authorization and/or credential information may be received. The requested information may be transmitted to the payment processing system after a payment

key code is received from the user via input device 108 or the user is otherwise authenticated (e.g., by entering a username and/or password on a computing device to which device 100 is connected). In some embodiments, different payment key codes may be associated with different financial accounts.

**[0043]** In some embodiments, m-commerce module 122 may be configured to provide credential and/or other information to process payments/transactions wirelessly and/or without device 100 being physically connected to another computing device. For example, wireless transceiver 106 may include a RFID device (e.g., transceiver or tag) configured to communicate wirelessly with a RFID terminal (e.g., a point-of-sale terminal in a retail or other type of business, a smartphone or other mobile computing device equipped with RFID, etc.). In some embodiments, the RFID device of device 100 may include a NFC tag (e.g., similar to a tag found on some credit cards to enable wireless near-proximity authorization of transactions by holding the card near a payment terminal). The user may hold device 100 near the RFID terminal of the payment system (e.g., within a predetermined communication distance associated with the RFID protocol) and enter a payment key code via input device 108. In various embodiments, the payment key code may be the same code or a different code from an access key code used to access device 100. Device 100 may be configured to verify the payment key code and, once verified, transmit the requested financial and/or credential information to the payment device. Using m-commerce module 122, device 100 may operate similar to a credit card or other financial instrument but may be more secure due to the encryption and other security features that prevent the data from being improperly accessed and used by an unauthorized person (e.g., if stolen). In some embodiments, the user may be enabled to select from any of multiple financial accounts (e.g., multiple debit or credit accounts) stored on device 100 when making a payment.

**[0044]** In some embodiments, m-commerce module 122 may be used to transmit information other than information used to complete transactions. For example, customers often carry various store-branded rewards or loyalty tags used to accumulate rewards points based on purchases and activities with a particular business (e.g., in a wallet, on a keychain, etc.). In some embodiments, account information associated with such rewards tags may be stored on device 100 and may be transmitted (e.g., wirelessly) to a payment system upon user entry of a

payment key code or separate rewards key code. Such a feature may allow a user to consolidate some or all of the user's rewards accounts into a single device.

**[0045]** In some embodiments, device 100 may be equipped with access control features such that device 100 can be used to access physical resources that are protected by access control devices. An access control module 118 may be configured to communicate with one or more access control devices that control access to physical resources and locations. For example, an electronic access control device may be used to control access to a door of a house, office, business, or other location, a car door, a door of a safe, or any other location or resource for which it is desirable to restrict access. A user may enter an access control key code to place device 100 into an access control mode, and device 100 may be operably connected (e.g., physically, electrically, communicatively, wirelessly, etc.) with the access control device and transmit credential information to the access control device. The access control device may authenticate the user based on the credentials and grant access to the protected location or resource. In some embodiments, different access control key codes may be associated with different access control devices and/or different protected locations and/or resources. In some embodiments, access control module 118 may be configured to communicate with the access control device via a wireless communication protocol, such as RFID, and access control module 118 may be configured to transmit credential information wirelessly to the access control device (e.g., when within a predetermined proximity of the access control device and a valid access control key code has been received from the user). The credential/authentication data and/or other access control data may be encrypted using encryption module 120 and securely stored in memory 104. In various embodiments, the access control key code may be entered by the user before or after device 100 has been placed within the proximity of the access control device. In some embodiments, the access control device may be configured to verify the legitimacy of the credentials by communicating over a network (e.g., network 140) with one or more security systems 144. For example, the user may deactivate a home security system by placing device 100 within proximity of a base station of the security system and entering the access control key code. Device 100 may transmit authentication information to the security system base station, and the authentication information may in turn be transmitted to a remote security database operated by a security

company to verify the legitimacy of the authentication information before the security system is disabled.

**[0046]** In various embodiments, users may be enabled to customize different key codes to apply to different functions and/or levels of data access. For example, a master key code may unlock all functions and data of device 100, a first user key code may unlock a first set of secure data on device 100 but not a second set of secure data, a second user key code may unlock the second set of secure data but not the first set, a guest key code may unlock certain data and functions of device 100 designated as “public” or unsecured information but not any secure information, etc. One or more access control key codes may be used to enable access via access control devices. One or more payment key codes may be used to provide financial-related information for enacting transactions. In some embodiments, a single key code may be used for multiple functions, such as access control, payments, and/or secure data access. In some embodiments, different resources and functions may be unlocked by different key codes. In some embodiments, device 100 may be associated with different users, and each user may have a set of data and functions to which the user is granted access, such that one or more key codes of a user are configured to unlock various data and functions to which the user has access. In some embodiments, the user may choose to not require a key code to be entered to access some or all of the data and/or functions of device 100 (e.g., a portion of memory 104 may be reserved for use of device 100 as a normal memory device, without security for that portion, the user may choose to require a key code for financial transactions but not for access control, etc.).

**[0047]** In some embodiments, file system 135 may be configured to keep a history of some or all of the activities performed using device 100. For example, file system 135 may keep a record of any access codes entered and when they were entered, any data transmissions to or from device 100, any access of data stored on device 100, any uses of device 100 to perform access control and/or payment activities, etc. The level of historical tracking performed by file system 135 may be configured by the user. Historical tracking may allow a user to determine whether any unauthorized use or access of device 100 or any data stored thereon has occurred (e.g., if device 100 is temporarily misplaced).

**[0048]** In some embodiments, device 100 may include a ruggedized housing configured to protect the various components of device 100 from damage. The housing may be durable, waterproof, dustproof, shock resistant (e.g., resistant to drops), resistant to damage from electrostatic discharge (ESD), etc. Device 100 may be fireproof and/or designed to be operable and/or storable within a wide range of temperatures (e.g., -40F to 150F). In some embodiments, the housing may be crush-resistant (e.g., may be able to withstand being run over by a car several times when connector 110 is in a retracted position). In some embodiments, device 100 may be tamper-resistant. For example, the housing of device 100 may be epoxy-filled, such that electronics are damaged or destroyed if the housing seal is forced open, and/or may be designed such that the processor 102 and/or memory 104 short-circuit if the housing is opened. In one embodiment, device 100 may have dimensions of approximately 2" x 0.5" x 0.25".

**[0049]** In some embodiments, device 100 may include an antivirus application configured to scan files and applications stored on device 100 for potential viruses and/or malware. In some embodiments, the antivirus application may be capable of performing virus-scanning in real-time or near real-time as files and applications are stored on device 100.

**[0050]** In some embodiments, device 100 may be configured to enable secure access to internet resources through a computing device operably connected to device 100 (e.g., through connector 110 and/or wireless transceiver 106). Internet access may be routed through a remote server (e.g., Master Lock Vault) and may be configured to allow secure and/or anonymous browsing and/or purchasing abilities. Data may be synchronized to the remote server, and transactions may be processed using data stored on the remote server and/or device 100. In some embodiments, secure internet access may be enabled by entering an access key code via input device 108. In some embodiments, device 100 may provide end-to-end encryption from device 100 through an intermediary device (e.g., a personal computer) to a remote server (e.g., Master Lock Vault) and/or to various web services, such as payment services, financial services, etc. (e.g., through the remote server). In some embodiments, device 100 may be configured to utilize secure channels (e.g., SSL, HTTPS) to transmit data. In some embodiments, device 100 may be configured to enable anonymous access to various network-

enabled services, such as financial services (e.g., through a remote server or gateway service such as Master Lock Vault).

**[0051]** In some embodiments, other devices may be used to unlock one or more features of device 100. For example, another device may be used to unlock data access, coupling device 116, extension of connector 110, and/or other features of device 100 upon entering a password or passcode on the other device. In various embodiments, the devices used to unlock the features may include, but are not limited to, a connected computing system, remote data storage system 146, a browser application (e.g., by accessing an Internet-enabled application on a remote server system), and/or a smartphone or other mobile computing and/or communications device (e.g., by accessing a website and/or by operating an application on the mobile computing device). In some embodiments, biometric input devices included on device 100 or other devices may be used to unlock certain features of device 100, such as an interactive voice response (IVR) unit that is configured to unlock portions of device 100 based on an audio passcode, a camera or other imaging device configured to unlock portions of device 100 based on image (e.g., face) recognition, and/or a fingerprint scanner configured to unlock portions of device 100 based on recognition of a fingerprint of an authorized user. In some embodiments, one or more input device or external device (e.g., biometric input devices) may be used to access features of device 100 such as access control to physical resources, payment authorization, encryption/decryption, unlocking of coupling device 116 and/or connector 110, and/or other features. In some embodiments, the features may be unlocked in a limited manner by devices other than input device 108, such as limitations based on the amount of times device 100 can be unlocked and/or a time/date range during which device 100 can be unlocked.

**[0052]** Referring now to FIG. 2, a block diagram of a storage device 200 is shown according to another exemplary embodiment. The storage device shown in FIG. 2 may be configured to implement features described with respect to device 100.

**[0053]** The storage device includes a microprocessor 228. The microprocessor 228 is connected to a flash or solid state memory 210, which may include encrypted data and/or credentials used in commerce and/or access control applications.

**[0054]** The storage device 210 includes two separate USB-based connectors 250, 252 that may be used to connect the device to external devices. One connector is a full-size USB connector 250, and the other connector is a mini-USB connector 252. Both connectors are driven by a USB driver circuit 244 configured to transmit and receive data and/or power signals through the connectors. The connectors 250, 252 may be extended and retracted by a retractor 254 (i.e., manually pushed, spring-biased, controllably locked/unlocked, etc.) of the storage device. A battery may be trickle-charged through the USB connectors 250, 252 using power received from a connected external device (e.g., computing device 260).

**[0055]** The storage device includes an encryption module 212 configured to implement one or more encryption algorithms and/or protocols. In some embodiments, the encryption protocols may include FIPS 214 and/or an AES encryption module 216. The device may support one or more types of encryption tunnels 218 or pipes through which data may be securely transferred. In some embodiments, the encryption tunnels may include a secure socket layer (SSL) 220 or HTTP secure (HTTPS) connection layer 224.

**[0056]** Access to data on the storage device may be controlled by a keypad including multiple keys that can be pressed in various sequences to enter different key codes. A keypad driver may be used to generate input signals based on the keys that are pressed, and the signals may be sent to the microprocessor for comparison to stored key codes to authenticate the user. Based on the authentication, a key code may unlock use of an access control module to enable access to physical resources that are secured by access control devices and/or a m-commerce application 226 to use the storage device to complete transactions. A timer circuit 234 may be used to implement an idle lockout function, such that the storage device is locked after a certain amount of time has passed since a last action was taken. The storage device 200 includes a RFID driver 240 and associated antenna 242 for transmitting and receiving signals to RFID systems (e.g., RFID readers). The RFID function may be used, for example, to communicate with access control devices and/or payment devices in the proximity of the storage device.

**[0057]** The storage device may include a LED 238 or other indicator configured to indicate whether the storage device has been unlocked (e.g., by entering a verified

key code) for use. In some embodiments, a green indicator may indicate that one or more functions have been unlocked for use and a red indicator may indicate that the device is locked and cannot be used until a valid key code is entered. In some embodiments, the storage device may include different or additional output devices, such as a display, multiple visual output indicators, a speaker, and/or other devices that may be configured to provide an indication of different authentication conditions. For example, a display or set of indicators may indicate that a general access code has been entered to give the user access to certain data on the storage device, but that the storage device is not yet enabled to provide transaction-related data or perform access control-related functions based on the current active access key. In some embodiments, the output indicator or indicators may notify the user of different mode settings or device states (e.g., encrypted, tampered with, unlocked, etc.). In some embodiments, a display may be used to allow the user to select from among multiple options or modes that may be used on the device. For example, in a payment mode, the display may be configured to display payment options (e.g., credit card, debit card, and/or prepaid card), and a selector switch may be used to cycle through the options and select a desired option when shown as an active option on the display. In various embodiments, the display may be or include a digital display (e.g., a 7-segment display), a LED display, a LCD display, or another type of display. LED 238 is shown as coupled to an LED driver 236.

**[0058]** The storage device 200 is shown to include a shackle 232 (e.g., padlock shackle, rigid shackle, flexible shackle, etc.) that can be used to physically couple the device to another object, such as a keychain or bag. In some embodiments, the shackle 232 may be locked using a blocking device that may include a driver circuit 202 and a solenoid device 230. The solenoid 230 may force the shackle 232 to remain in a locked position until a valid key code is entered on the keypad 206, at which point the solenoid may disengage and allow the shackle to be opened. This may reduce the risk of theft of the storage device.

**[0059]** In some embodiments, the storage device 200 may be configured to be connected to systems (e.g., systems 272-278) through a network connection such as an Internet connection. The storage device 200 may be connected through the Internet 270 through an intermediary computing device 260 to which the storage device is connected (e.g., through the USB connectors or wirelessly). The storage

device 200 may be connected to any of a variety of different systems and/or services, such as remote storage systems 272 (e.g., Master Lock Vault), financial providers and/or services 274, 276, 278, 280 (e.g., banks, PayPal, credit card companies, Google Wallet, etc.), Internet services (e.g., social networks, such as Facebook), and/or other systems and/or services. In some embodiments, the user may be authenticated on these services using credential data stored on the storage device 200. In some embodiments, the user may connect to various network-enabled services through a gateway service or remote server (e.g., Master Lock Vault). In some such embodiments, the gateway service or remote server may enable a user to perform certain actions on other network-enabled services anonymously (e.g., using information stored on the storage device and/or by the gateway service or remote server).

**[0060]** Referring now to FIG. 3, a flow diagram of a process 300 for enabling access to secure data stored on a storage device is shown according to an exemplary embodiment. One or more operations of process 300 may be performed using various features and/or components of device 100 and/or the storage device illustrated in FIG. 2.

**[0061]** An access key may be received from a user via an input device of a storage device (305). In an exemplary embodiment the input device may be a set of soft keys (e.g., provided by a touch screen). In other embodiments, the input device may be a hardware keypad. In yet other embodiments the input device may be a biometric scanner, a dial, or a set of varying input mechanisms.

**[0062]** The storage device may be configured to compare the received access key to access key data stored in a memory of the storage device (310). If the access key does not match a stored access key associated with the user, the storage device may deny access to data stored in the memory (315). The storage device may be configured to determine if a number of failed attempts at providing access keys has exceeded a threshold level (320). If the number of failed attempts has not exceeded the threshold level, the storage device may wait to receive another access key from the input device. If the number of failed attempts has exceeded the threshold level, in some embodiments, the storage device may be configured to destroy some or all of the data stored in the memory (325).

**[0063]** If the access key matches a stored access key for the user at operation 310, the storage device may be configured to enable access to the data by a connected device (e.g., a computing device) (330).

**[0064]** According to an exemplary embodiment, the data which is enabled for access may be a key for accessing a remote system. The key for accessing a remote system may be generated in response to a correct access key entry. The key for accessing a remote system may be encrypted, combined with other data, generated using a public or private key, or otherwise prepared for transmission and authentication by the remote system.

**[0065]** In some embodiments, the storage device may include an idle timer configured to track an amount of time that has elapsed since a last activity was performed using the storage device (335). If the idle timer has not exceeded an idle timeout threshold, the storage device may continue to permit access to the stored data. If the idle timer has exceeded the threshold, the storage device may require the user to re-authenticate before data can be accessed.

**[0066]** Referring now to FIG. 4, a flow diagram of a process 400 for enabling wireless access to secure data stored on a storage device is shown according to an exemplary embodiment. One or more operations of process 400 may be performed using various features and/or components of device 100 and/or the storage device illustrated in FIG. 2.

**[0067]** A request for access to data stored on a storage device may be received by the storage device over a wireless connection (405). In some embodiments, the storage device may be configured to determine an identity associated with the requesting device (410) and to verify if the identity is legitimate (e.g., based on stored data regarding trusted devices with which the storage device may communicate) (415). For example, if the requesting device is an access control device or payment processing device, the storage device may be configured to use identification information transmitted with the request to determine if the requesting device is associated with a legitimate access control or financial provider to reduce the risk of transmitting sensitive information to an unauthorized entity. If the identity is not associated with a legitimate requesting device, the request for data access may be denied (420).

**[0068]** If the identity is verified as legitimate, the storage device may determine whether a user access key has been received and verified (425). If an access key

has already been received, the requesting device may be granted access to the data (430). If an access key has not yet been received, the storage device may wait to receive an access key from the user via the input device of the storage device (435). Once an access key is received, the storage device determines whether the access key matches a stored access key for the user (440). If the received access key does not match a stored access key, the request is denied. If the received access key matches a stored access key, the access request is granted.

**[0069]** Referring now to FIG. 5, a flow diagram of a process 500 for enabling access to a resource secured by an access control device (e.g., a lock for a home or business door, a padlock, a lockbox, a commercial terminal, a payment terminal, etc.) using a storage device (e.g., a USB flash drive, a key fob having features described herein, etc.) is shown according to an exemplary embodiment. One or more operations of process 500 may be performed using various features and/or components of device 100 and/or the storage device illustrated in FIG. 2.

**[0070]** A storage device is configured to detect when an access control device is in proximity of the storage device (e.g., using a RFID transceiver or tag) (505). The access control device may be configured to secure access to any location or resource, such as a home or business, a car, a safe, an account, etc. The storage device is configured to receive an access key from a user via an input device (510) and to determine whether the received access key matches an access key configured to approve access to the location/resource protected by the access control device (515). If the access key does not match a stored access key, the storage device is configured to deny access to the protected resource/location (520). If the access key matches a stored access key, the storage device is configured to transmit a command and/or data (e.g., credential or authentication information) to the access control device that causes the access control device to grant access to the protected resource/location (525). The stored access key may be provided in addition to other credential or authentication information. In an exemplary embodiment, the stored access key is encrypted for transmission to the protected resource/location.

**[0071]** In other embodiments, the stored access key is never actually sent to the protected resource/location. Process 500 can advantageously be viewed as providing multi-factor authentication: the user must both have the storage device

(one factor) and the access key (a second factor). In alternative embodiments yet further factors may be used to provide additional levels of security. For example, a user may be required to enter a separate passcode on the side of the secure location or resource.

**[0072]** According to an exemplary embodiment, data to be transmitted from the storage device is encrypted using PGP encryption (or another encryption method) by encrypting the data using a random or pseudorandom key. The random or pseudorandom key is encrypted using RSA and a public key (associated with the receiver and pre-stored in the storage device). The receiving system can then decrypt the message using the receiving system's private key. Using the decrypted key, the data of the message from the storage device can be decrypted. Such a process may be triggered based on correct entry of the access key at the storage device's keyboard. Correct entry of the access key at the storage device's keyboard, therefore, may not only enable the hardware (e.g., a USB interface), but also may trigger the generation of a key and data for providing to a remote source. The key and data may be part of an encrypted data package for transmission to a remote source for authentication or for secure transmission.

**[0073]** In an exemplary embodiment, the present invention relates to a method for controlling access to first data on a portable electronic memory device. The method includes temporarily generating and exposing second data (e.g., a key or other payload data) for providing to a remote authenticator (e.g., remote server) in response to entry of a correct user input sequence at a user input device (e.g., the keypad on the USB flash drive). Temporarily exposing the data may include, for example, enabling the USB flash drive for operation with a local computing resource, generating a file containing the key or other authentication information, and exposing the file to reading and uploading by the local computer. In an exemplary embodiment, therefore, a user browsing on a website requiring an authentication may be instructed to upload an authentication file to the website server (e.g., before the user can transfer a large sum of money, before the user can access secure files in an online "vault"). The authentication file may not be available (or even generated) until the user enters the correct key combination on the USB flash drive, plugs the USB flash driver into the user's laptop, and uploads the file that was made available via the key entry. Using such a method, the user may advantageously need no fewer than three factors of information: (1) the USB

drive itself, (2) a correct access key combination, and (3) login credentials to the online website to which the upload of the authentication file can take place. In an exemplary embodiment, because the authentication, generation, and exposure of the file happens on the USB drive itself and not the local computer, no special software needs to be included on the local computer. Thus, the USB drive may be used to help provide three-factor authentication to the remote resource from any internet connected local computer and without any special software. The authentication file can be encrypted using PGP and/or the steps described above. Most browser software allows a local file to be selected for upload to a remote server. According to an exemplary embodiment, rather than file upload, the file generated on the flash drive includes a text string which can automatically or manually be copied and pasted or otherwise provided into a text field for authentication.

**[0074]** At the remote authenticator, user permissions to the user's browsing session (e.g., at the local computer) can be granted in response to a determination that the provided data (whether by upload or text entry) is authentic. The provided data may be encrypted. The remote authenticator may use a key (e.g., a private key, a key previously associated with the USB drive) to decrypt the data received from the portable electronic device. The remote authenticator may check the contents of the decrypted data to determine whether or not the second data is authentic. Only if the encrypted file is successfully decrypted and the contents are authentic (the contents may contain a user passcode), may the remote authenticator grant access to the user's computer.

**[0075]** Referring now to FIG. 6, a flow diagram of a process for authorizing a transaction using a storage device is shown according to an exemplary embodiment. One or more operations of process 600 may be performed using various features and/or components of device 100 and/or the storage device illustrated in FIG. 2.

**[0076]** A storage device is configured to detect when an payment processing device is in proximity of the access control device (e.g., using a RFID transceiver or tag) (605). For example, a proximity-based payment processing device may be located at a checkout of a retail store. The storage device is configured to receive a payment key from a user via an input device (610) and to determine whether the received payment key matches an payment key configured to authorize the

provision of financial-related information to the payment processing device (615). If the payment key does not match a stored payment key, the storage device is configured to reject the transaction (620). If the payment key matches a stored payment key, the storage device is configured to transmit financial and/or credential data to the payment processing device for use in consummating the transaction (625).

**[0077]** Referring now generally to FIGS. 7 through 13B, various illustrations of example storage device are shown according to various illustrative embodiments. Features shown with respect to any individual exemplary embodiment generally may be utilized with any other exemplary embodiment described herein. The various illustrated exemplary embodiments may incorporate features described with respect to the exemplary embodiments shown in FIGS. 1 through 6. For example, in some embodiments, a RFID tag (e.g., a NFC tag) may be included on a portion of the device (e.g., a back portion) and a keypad may be included on another portion of the device (e.g., a front portion).

**[0078]** Referring now to FIGS. 7A-13D, exemplary embodiments of storage devices are shown. The storage device includes a USB connector that may be retracted into the main body or housing of the storage device using a slider switch on the side of the device. The storage device includes a six digit keypad that can be used to enter key codes. In some exemplary embodiments the USB connector is protected by a cap that is secured by an elastic band. A key ring may be attached to a rear slot. The device may include a ten digit keypad that also has an enter key for indicating when entry of a key code has been completed and a clear key for clearing or restarting entry of a key code. A LED indicator bar may be provided about the periphery of the device to indicate whether the device is currently locked or unlocked. As illustrated in FIG. 7B, the storage device may include perforated metal surrounding the side of the housing and a water tight cover cap to protect the USB connector.

**[0079]** According to exemplary embodiments, the storage device may include a keypad having partially recessed keys. This may reduce the risk of the keys accidentally being pressed (e.g., in a pocket). A retractable cover may be provided which can be retracted when connecting the device to an external device or advanced to protect the USB connector. A cover door (e.g., a flip-down door) may

cover an end of the USB connector when in a closed position and may be weather-resistant.

**[0080]** In some embodiments, the storage device may include rocker switches having one position associated with one digit and another position associated with another digit. The device may have a carabineer-style coupling connector for connecting the device to another object. In some embodiments, the coupling connector may be locked until a release key code is entered on the rocker switches. The keypad of various exemplary embodiments may be implemented using a variety of different keypad types, such as a numerical keypad, a directional keypad (e.g., using a combination of arrow presses), rocker switches, etc. In some embodiments, the keypad may be a directional keypad where access key codes are entered as a sequence of arrow presses. In some embodiments, the user may select a specific letter or number illustrated on the face of a device by rotating a circular portion of the user interface until the arrows point at the desired letter/number. In some embodiments, the circular portion may be touch-sensitive, and the user may run a finger clockwise or counter-clockwise around the circular portion until a desired letter/number is selected (e.g., until an indicator, such as an LED, under the letter/number is activated). In some embodiments, once the desired key code has been entered, the button in the center may be pressed to enter the key code. FIG. 13B illustrates a possible size of the storage device and use of the device while connected to a computer and on a keychain, according to an exemplary embodiment.

**[0081]** In some embodiments the storage device includes a housing that is shaped similar to a padlock. In other embodiments the storage device has all of the structural components of a padlock and can operate as a padlock. In various exemplary embodiments, the storage device may include a housing with a tapered form. A directional keypad may be included on the front of the storage device, and a sliding retractor switch may be included on the rear side of the storage device for extending and retracting a USB connector. A USB connector may extend out of a bottom portion of the storage device. The front of the storage device also includes a status LED to indicate a status of the storage device (e.g., unlocked or locked), and the storage device includes a carabineer coupling attachment. The storage device may include a weather resistant door to protect the USB port when retracted. In some embodiments, the weather resistant door may include one or

two door pieces that may flip down when the USB port is recessed to protect the USB port from weather and/or other damage and may flip up when the USB port is extended. In some embodiments, the door may be locked into a closed position until an appropriate access code is entered via the keypad (e.g., to help prevent unauthorized use). In some embodiments, the storage device may include a stainless steel color such that the storage device appears similar to a metallic padlock.

**[0082]** In some exemplary embodiments, a shackle or clip (e.g., carabineer) may also serve as a retractor device for a retractable connector (e.g., a USB port). For example, a shackle may be configured such that it can be pushed into and pulled out of a recess inside a body of the storage device. In some embodiments, when the shackle is pushed into the recess, the connector may be extended into a use configuration, and when the shackle is pulled out of the recess, the connector may be retraced back into the body of the storage device and into a protected configuration. In some embodiments, one or both of the ability to push the shackle to extend the connector and open a clasp on the shackle may be locked until an appropriate access key code is entered on a keypad or other input device of the storage device.

**[0083]** Various other exemplary embodiments may include various features described above but modify selected features, such as form factor, connector placement, etc. For example, in some exemplary embodiments, the storage device may be configured to operate as a watch and may be connectable to a watch band. The storage device may include a display configured to display a current time and/or other features typically associated with a digital watch. A wireless transceiver, such as a RFID reader or tag, may be located near the display or face of the watch to allow the wireless function to be used while the device is worn on a wrist.

**[0084]** Another exemplary embodiment may include a larger storage device that may be constructed from solid state materials and may include a rechargeable battery trickle-charged through a USB port. The storage device may be portable and usable for storage and secure internet activities and/or commerce. In some embodiments, the storage device may have a form factor similar to a portable hard drive device. In some embodiments, the storage device may incorporate a wireless transceiver that may be configured to implement a one button modem

synchronization function with a wirelessly connected computer and/or a remote storage device. The device may have a rechargeable battery and may include a permanent electrical power connection (e.g., a wall socket adapter). In some embodiments, the device may be large enough to securely store objects such as physical papers, jewelry, etc. (e.g., may be similar in size, form factor, and/or some functions to a small safe). In some such embodiments, the device may include an integrated paper scanner that is synchronized to the storage of the device and/or to a remote storage device.

**[0085]** In some exemplary embodiments, a storage device may be configured such that two storage devices may communicate with one another in a peer-to-peer manner, either directly or through an intermediary computing device to which the storage devices are operably connected (e.g., a connected computing device and/or a remote server, such as Master Lock Vault). In some embodiments, the two storage devices may communicate directly with one another wirelessly, such as using a WiFi, Bluetooth (e.g., OBEX protocol), RFID (e.g., NFC), or other connection between the devices. A key code may be entered on each of the devices to indicate that the users of both devices authorize the communication, and once the key codes have been entered, the devices may share data. In some embodiments, data files may be shared between the two devices. In some embodiments, payment data (e.g., credit, debit, PayPal, etc.) may be shared between the devices. For example, money may be transferred from an account associated with secure financial data stored on a first device to another account associated with data stored on the second device, such that the devices can be used to transfer funds from a user of the first device to a user of the second device. In some embodiments, access control data may be shared between the devices. For example, a user of a first device may transmit authorization data to a user of a second device authorizing the user to access certain protected resources using authentication information stored on the first device.

**[0086]** The construction and arrangement of the systems and methods as shown in the various exemplary embodiments are illustrative only. Although only a few embodiments have been described in detail in this disclosure, many modifications are possible (e.g., variations in sizes, dimensions, structures, shapes and proportions of the various elements, values of parameters, mounting arrangements, use of materials, colors, orientations, etc.). For example, the position of elements

may be reversed or otherwise varied and the nature or number of discrete elements or positions may be altered or varied. Accordingly, all such modifications are intended to be included within the scope of the present disclosure. The order or sequence of any process or method steps may be varied or re-sequenced according to alternative embodiments. Other substitutions, modifications, changes, and omissions may be made in the design, operating conditions and arrangement of the exemplary embodiments without departing from the scope of the present disclosure.

**[0087]** The present disclosure contemplates methods, systems and program products on any machine-readable media for accomplishing various operations. The embodiments of the present disclosure may be implemented using existing computer processors, or by a special purpose computer processor for an appropriate system, incorporated for this or another purpose, or by a hardwired system. Embodiments within the scope of the present disclosure include program products comprising machine-readable media (e.g., tangible and/or non-transitory) for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, flash memory, or any other medium which can be used to carry or store desired program code in the form of machine-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer or other machine with a processor. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a machine, the machine properly views the connection as a machine-readable medium. Thus, any such connection is properly termed a machine-readable medium. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions.

**[0088]** Although the figures may show a specific order of method steps, the order of the steps may differ from what is depicted. Also two or more steps may be performed concurrently or with partial concurrence. Such variation will depend on the software and hardware systems chosen and on designer choice. All such variations are within the scope of the disclosure. Likewise, software implementations could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various connection steps, processing steps, comparison steps and decision steps.

What is claimed is:

1. A portable electronic memory device, comprising:
  - a housing;
  - non-transient computer-readable media within the housing;
  - a plurality of key buttons disposed upon the housing and configured to allow entry of a security code by a plurality of keystrokes;
  - a communications interface for communication with external electronics that are not a part of the portable electronic memory device;
  - a circuit which has a locked state and an unlocked state, wherein the correct entry of the security code is required to enter the unlocked state, wherein the unlocked state permits access to first data of the non-transient computer-readable media which is inaccessible in the locked state, and wherein the entry of the security code also causes second data comprising a key to be generated and made available to the external electronics via the communications interface.
2. The portable electronic memory device of Claim 1, wherein the communications interface is a universal serial bus (USB) interface.
3. The portable electronic memory device of Claim 1, further comprising:
  - a padlock shackle extending from the housing and wherein the housing comprises a blocker solenoid for locking or unlocking the padlock shackle.
4. The portable electronic memory device of Claim 1, wherein the circuit encrypts the first data and the key for transmission via the communications interface.
5. The portable electronic memory device of Claim 1, wherein the circuit is configured to associate different keypad combinations with a different activities;
  - wherein a first keypad combination is used to transition the device between the locked state and the unlocked state; and wherein a second keypad combination generates authenticating data for at least one of: (a) a physical device entry code, (b) a commercial transaction, (c) authentication with a remote server.

6. The portable memory device of Claim 1, wherein the circuit is configured to associate different keypad combinations with different pieces of data to be selectively secured and made available for transmission via the communications interface.
7. The portable electronic memory device of Claim 1, wherein making the data comprising the key available to the external electronics comprises permitting the key to be forwarded as a text string.
8. The portable electronic memory device of Claim 1, wherein making the data comprising the key available to the external electronics comprises generating a file containing the key in the non-transient computer-readable media and permitting the key to be uploaded to a remote server via the electronics.
9. The portable electronic memory device of Claim 1, wherein the circuit is configured to transmit the data comprising the key to the external electronics via the communications interface in response to input received from the plurality of key buttons.
10. The portable electronic memory device of Claim 1, wherein the circuit comprises a timer and wherein the timer deletes the data after a period of time counted using the timer.
11. The portable electronic memory device of Claim 1, wherein the circuit comprises an evaluation module and a timer and wherein the evaluation module deletes the key if a valid request for the key is not received with a period of time counted using the timer.
11. The portable electronic memory device of Claim 1, wherein the circuit encrypts the first data stored on the memory device using the key generated by entry of the security code.

12. The portable electronic memory device of Claim 1, wherein the circuit receives a second key via the communications interface and encrypts the key generated by entry of the security code using the second key;  
wherein the circuit makes the encrypted first data and the encrypted key available for transmission via the communications interface.
13. The portable electronic memory device of Claim 1, wherein the communications interface is an active RFID interface.
14. The portable electronic memory device of Claim 1, wherein the communications interface is a passive RFID interface.
15. The portable electronic memory device of Claim 13 or 14, wherein the generated key is made available for reading or writing via the RFID interface.
16. The portable electronic memory device of Claim 1, wherein the circuit maintains a history of unlock, lock, and/or transfer events in the non-transient computer readable media.
17. The portable electronic memory device of Claim 1, wherein the circuit controls a solenoid to allow or prevent the communications interface from being extended outside of the housing.
18. The portable electronic memory device of Claim 1, wherein the circuit comprises a tamper detection module configured to determine whether the housing has been compromised and to cause the first data to be destroyed in response to a determination that the housing has been compromised.
19. The portable electronic memory device of Claim 1, further comprising:  
an electronic display coupled to the housing;  
wherein the circuit controls the display to cause at least one of a tamper alert and a keypad entry status to be indicated via a state change of the display.

20. A method for controlling access to a remote server using a portable electronic memory device, comprising:
- receiving an access request at a portable electronic device from the remote server;
  - receiving user input via a keypad on the portable electronic device;
  - checking the keypad entry on the portable electronic device and providing an authentication response to the remote server if the keypad entry is verified;
  - providing access to the remote server by a computing device associated with the user.
21. The method of Claim 20, wherein the computing device is a local computing device in communication with the portable electronic device locally and in communication with the remote server via a wide area connection.
22. The method of Claim 21, wherein the portable electronic memory device is a USB dongle having the keypad and memory local to the USB dongle.
23. The method of Claim 22, wherein the access controlled is virtual private network access between the local computing device and the remote server.
24. A method for controlling access to first data on a portable electronic memory device or on a remote resource, comprising:
- temporarily generating, encrypting, and exposing second data for providing to a remote authenticator in response to entry of a correct user input sequence at a user input device;
  - at the remote authenticator, granting user permissions to the first data in response to a determination that the second data is authentic;
  - wherein the remote authenticator uses a key stored at the remote authenticator and associated with the portable electronic memory device to decrypt the second data received from the portable electronic device;
  - checking the contents of the decrypted data to determine whether or not the second data is authentic.

25. The method of Claim 24, wherein the remote authenticator requires a separate log-in by the user such that multi-factor authentication is required for the remote authenticator to grant access.
26. The method of Claim 24, wherein the portable electronic memory device is a USB flash drive.
27. The method of Claim 24, wherein the portable electronic memory device is a key fob and does not primarily function as a USB flash drive.
28. The method of Claim 24, wherein the input device is a hardware key pad.
29. The method of Claim 24, wherein the input device is a touch screen providing soft keys.

1/15

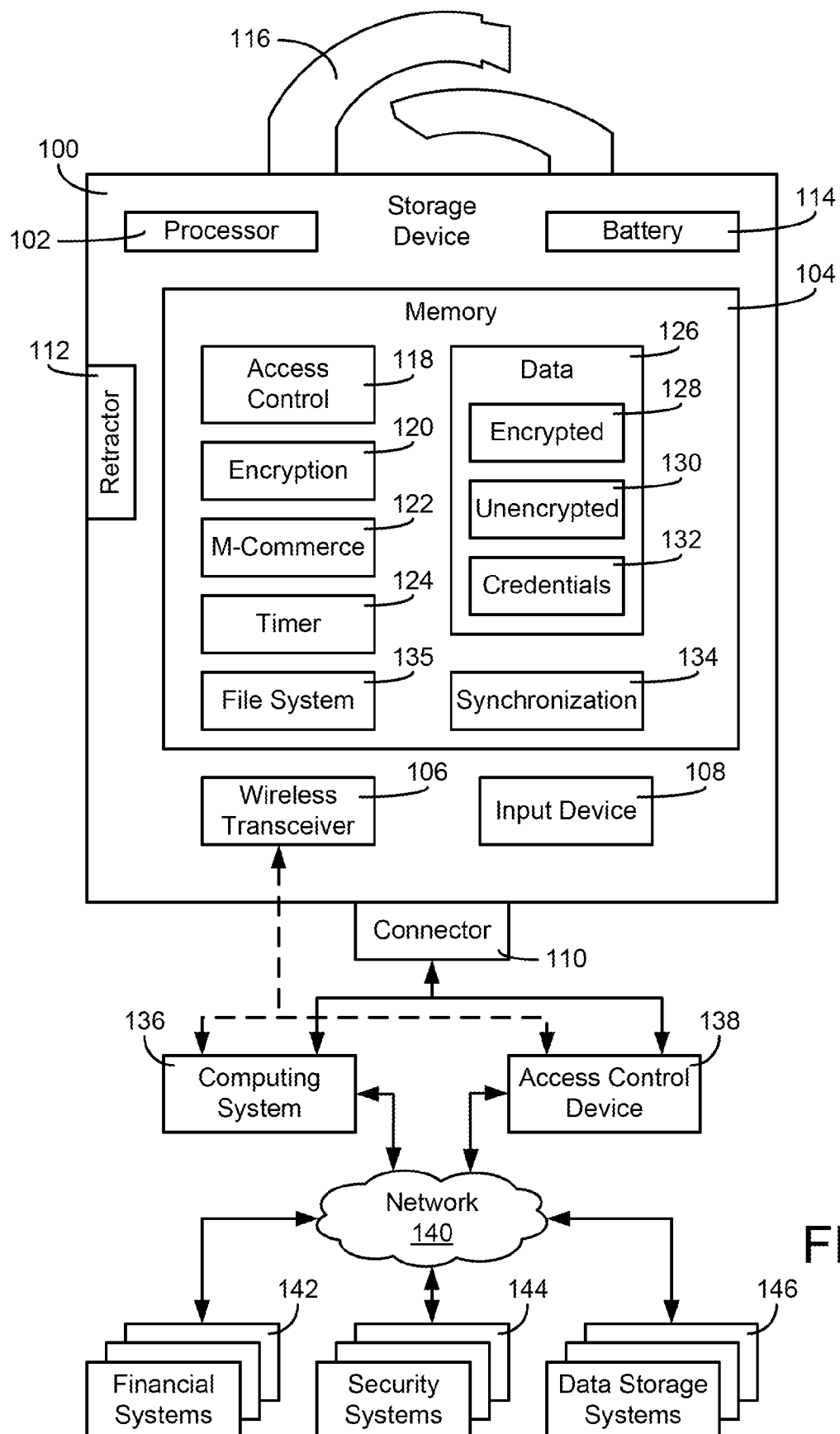


FIG. 1

2/15

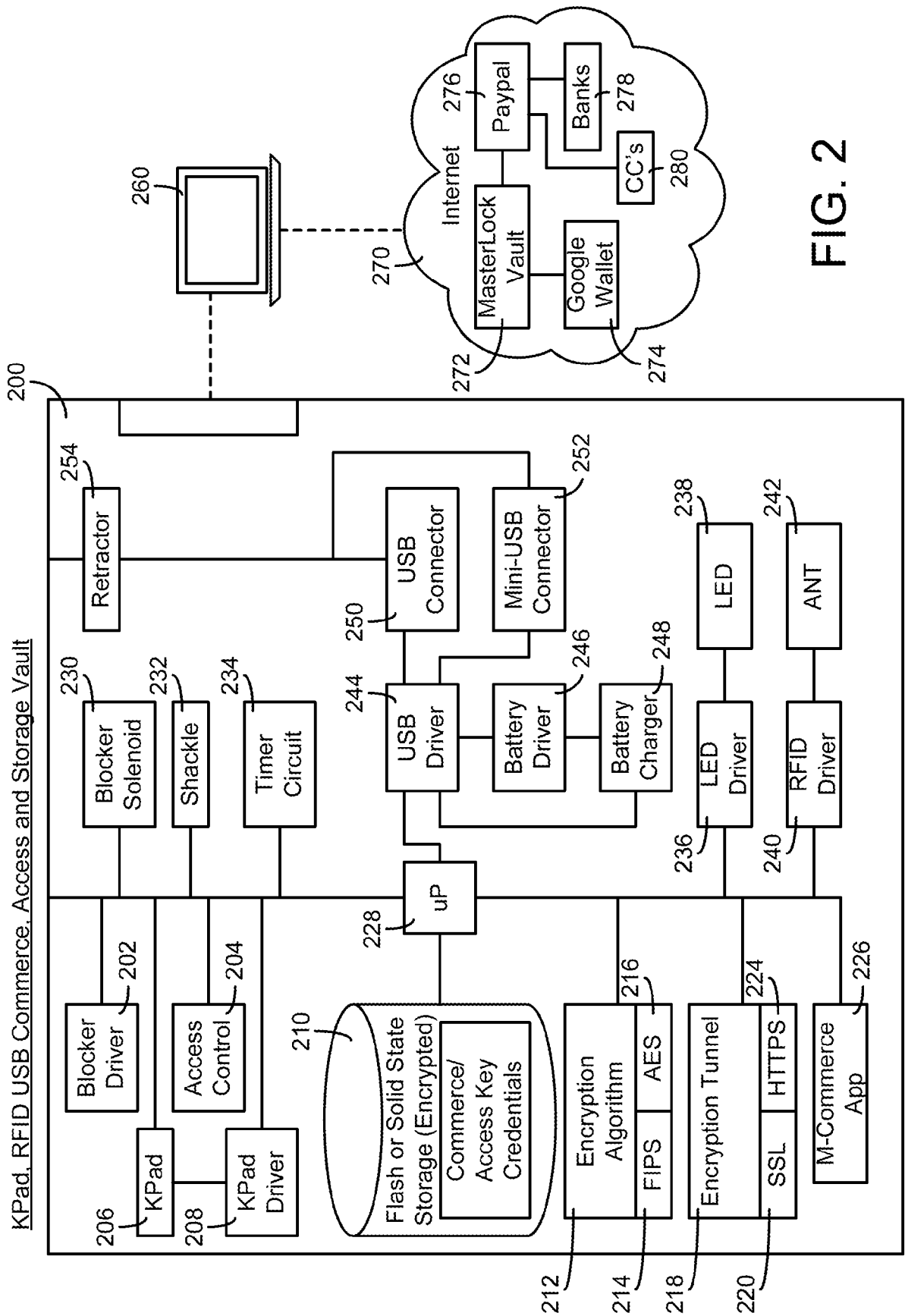


FIG. 2

3/15

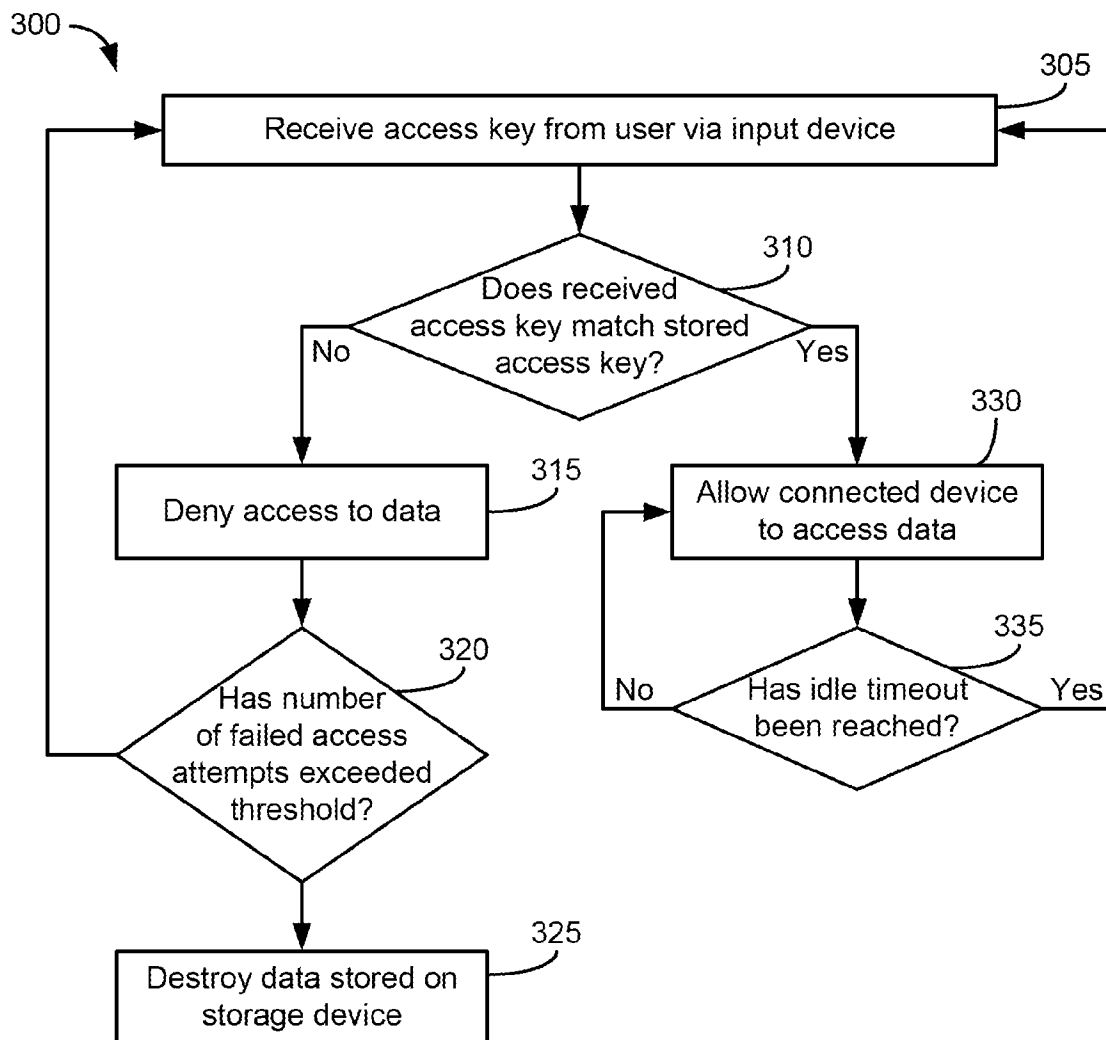


FIG. 3

4/15

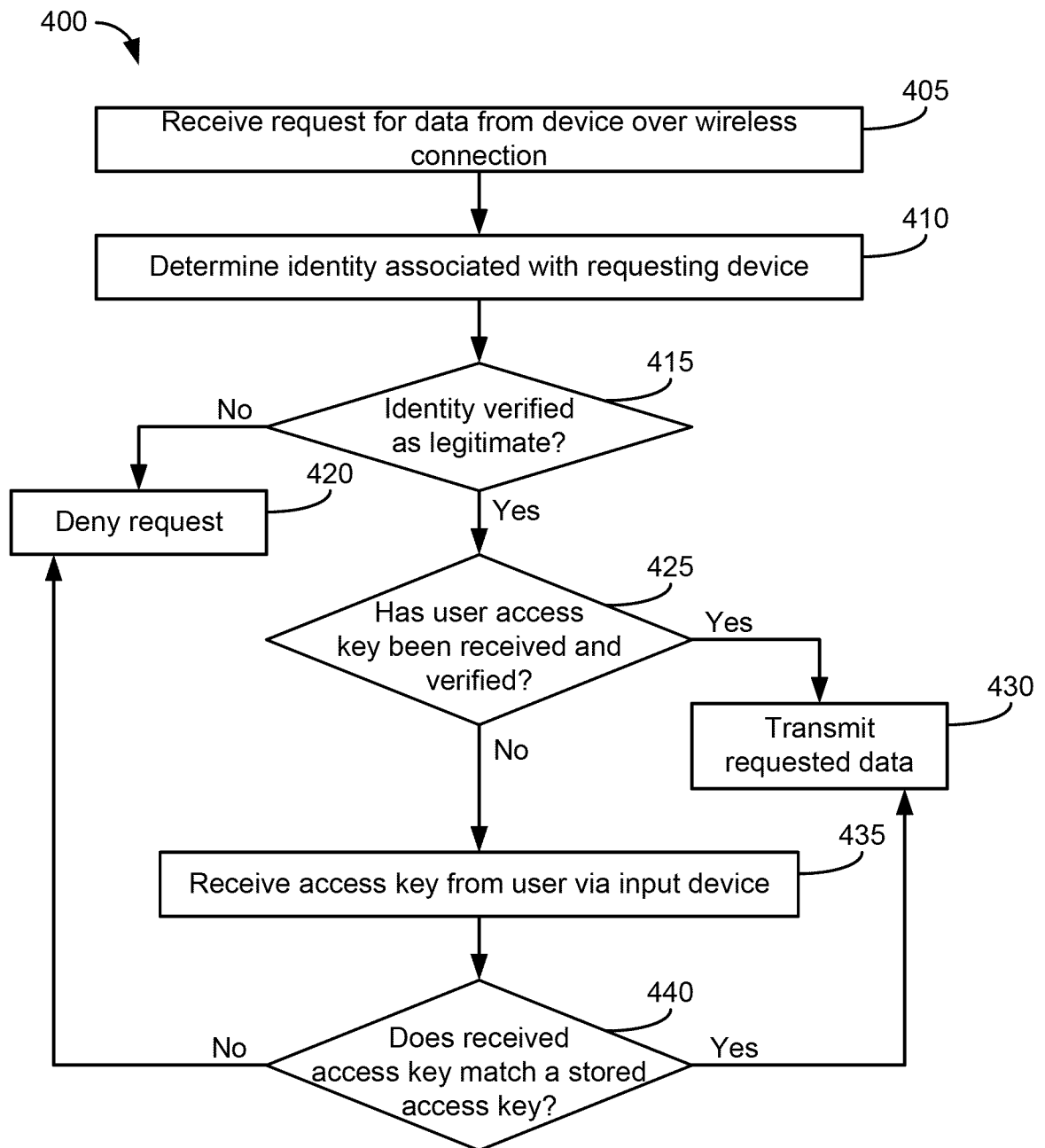


FIG. 4

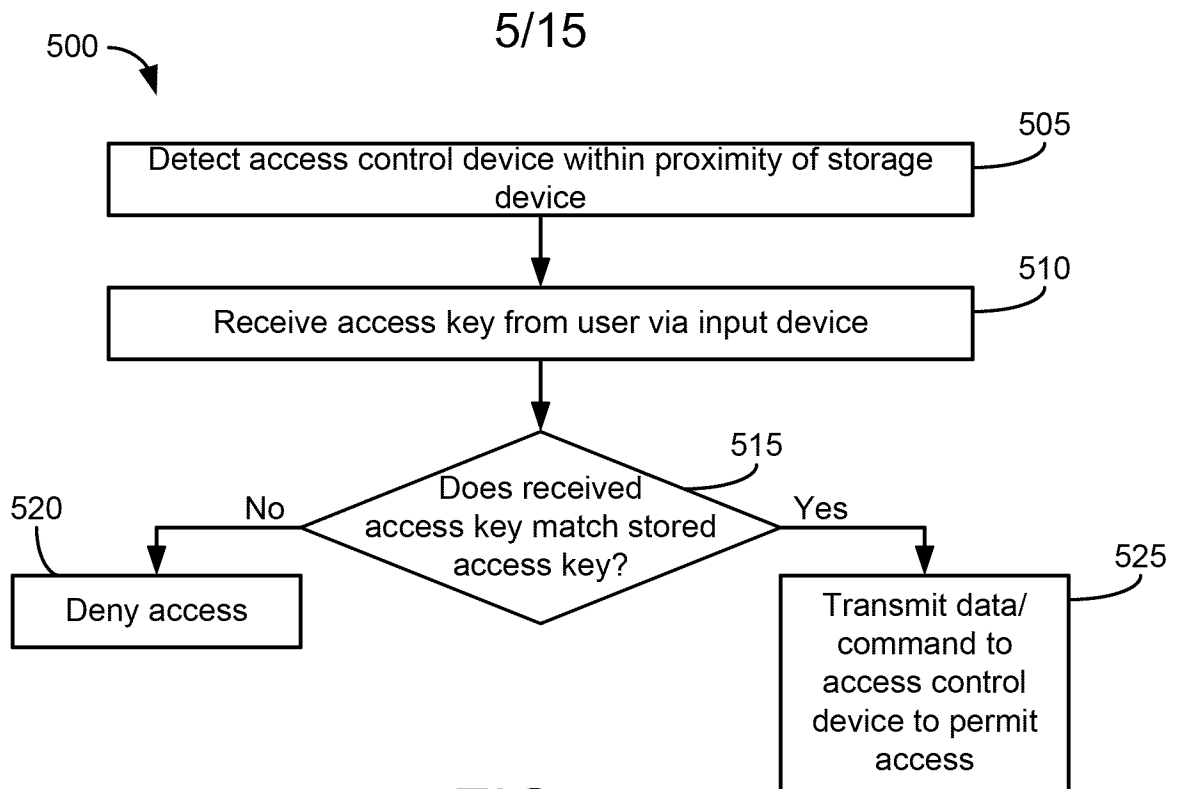


FIG. 5

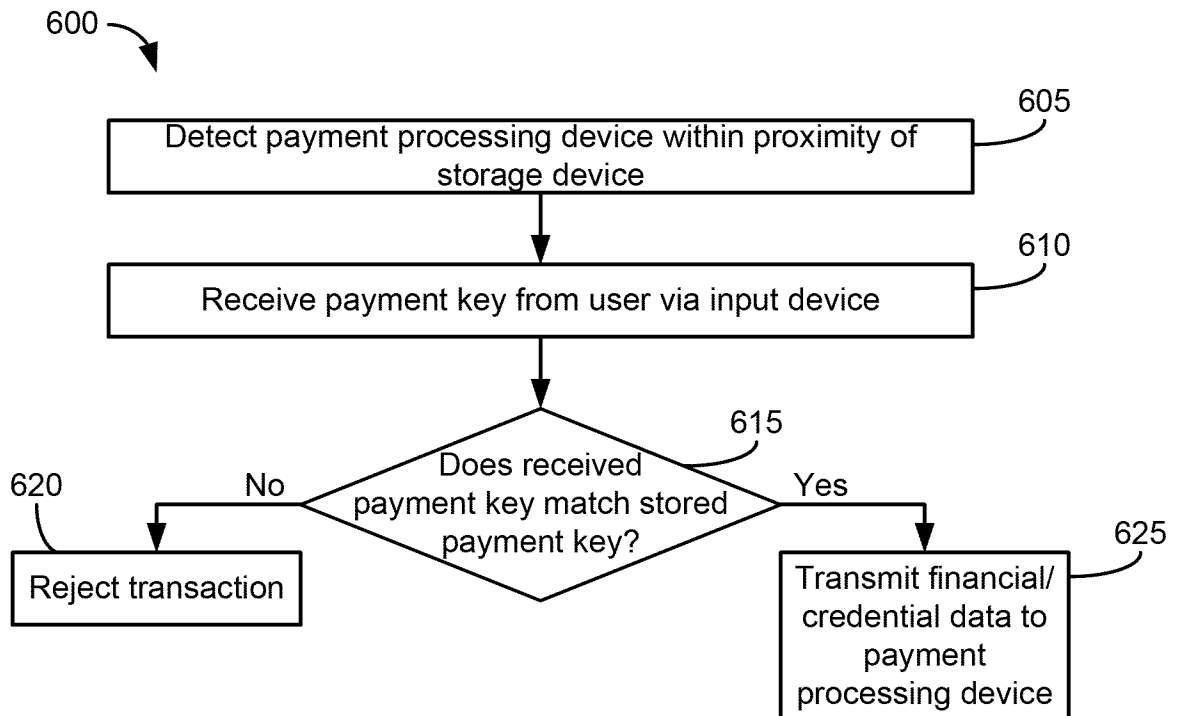


FIG. 6

6/15

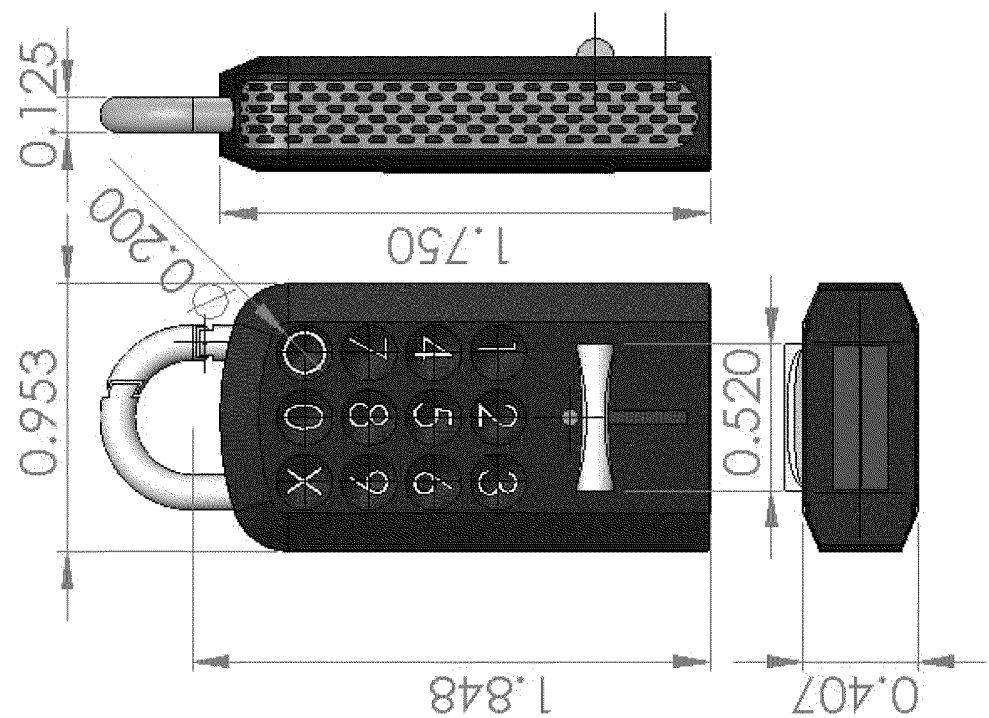


FIG. 7B



FIG. 7A

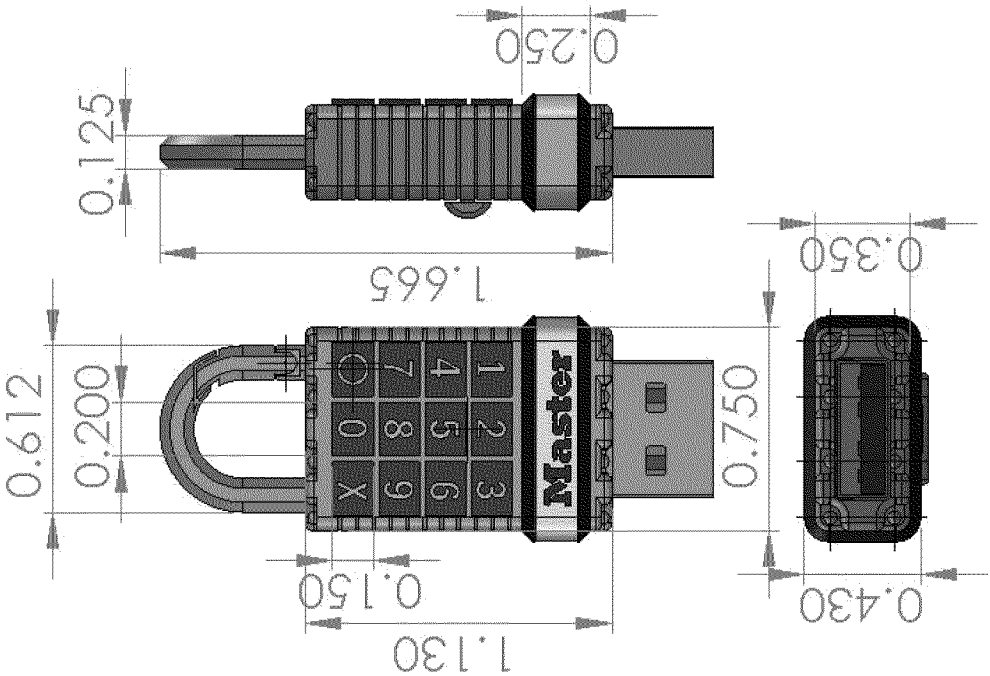


FIG. 8B



FIG. 8A

8/15

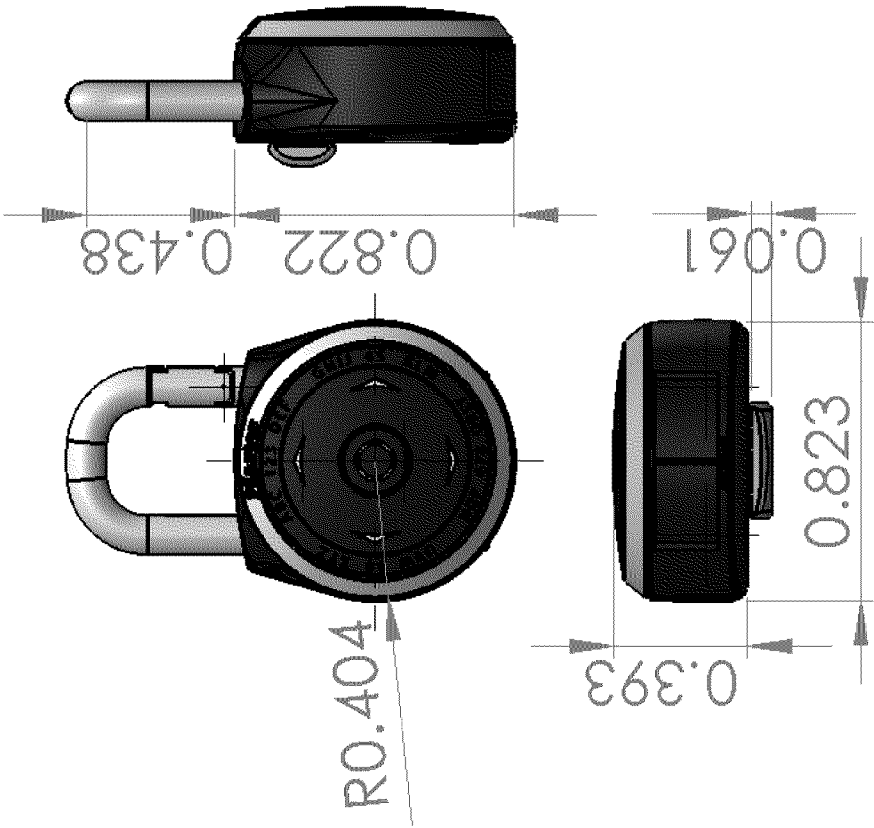


FIG. 9B

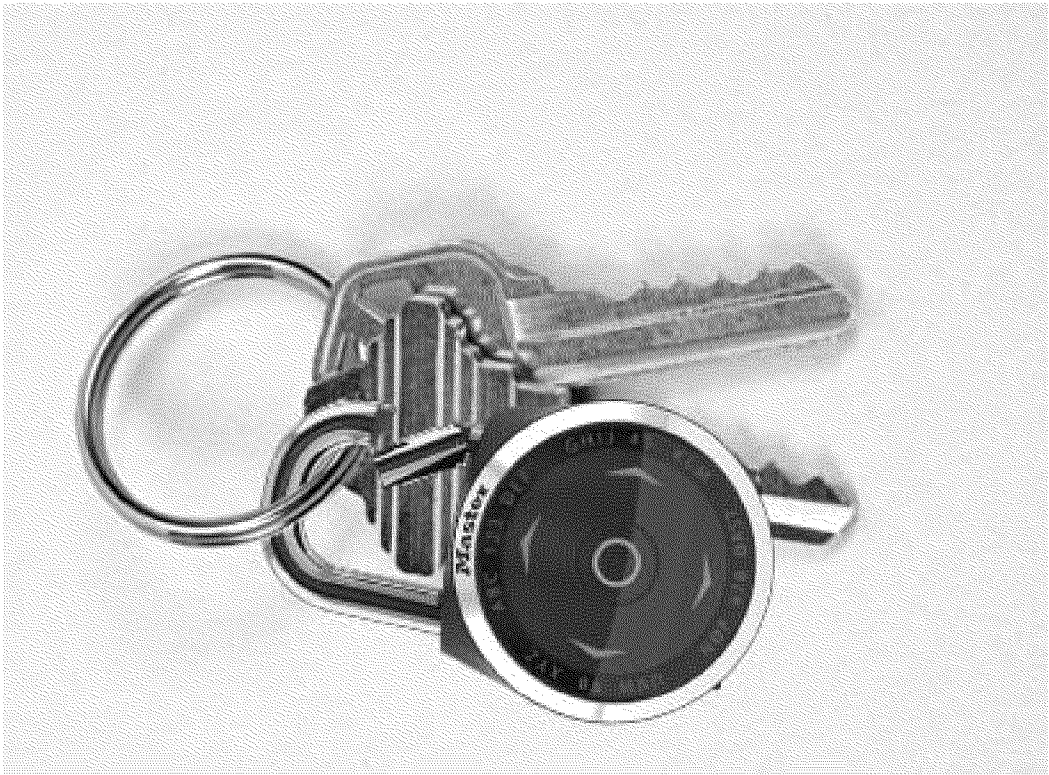


FIG. 9A

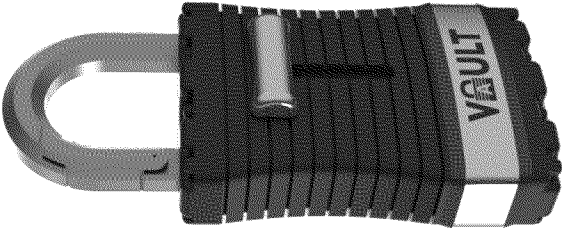


FIG. 10C



FIG. 10B



FIG. 10A

10/15



FIG. 10F



FIG. 10E



FIG. 10D

11/15

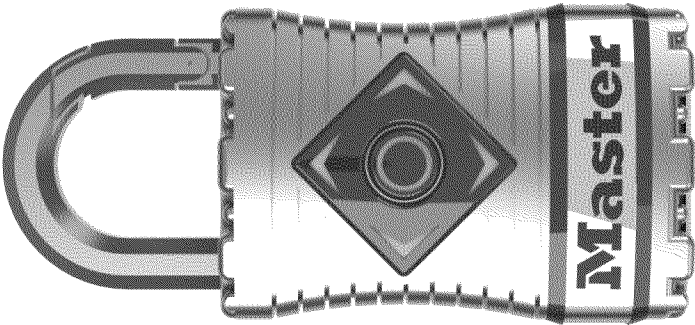


FIG. 10H



FIG. 10G

12/15

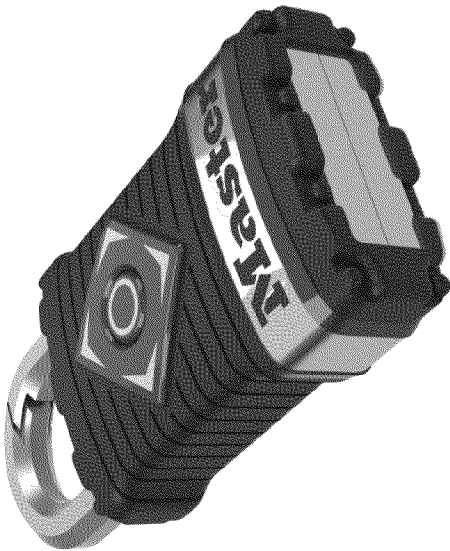


FIG. 11C



FIG. 11B

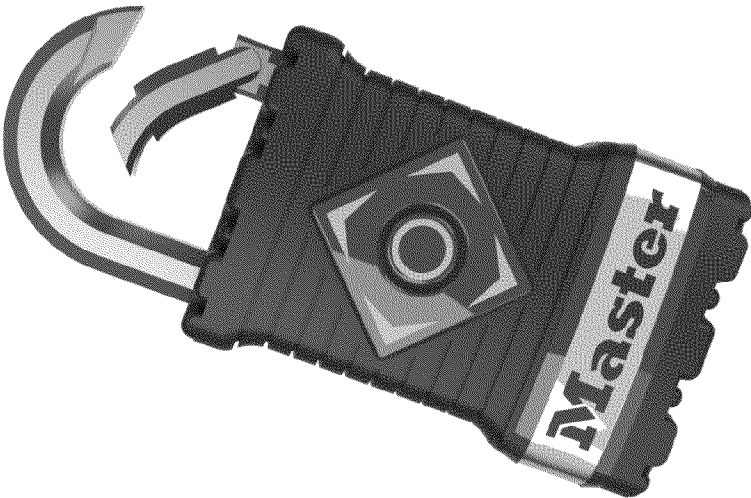


FIG. 11A

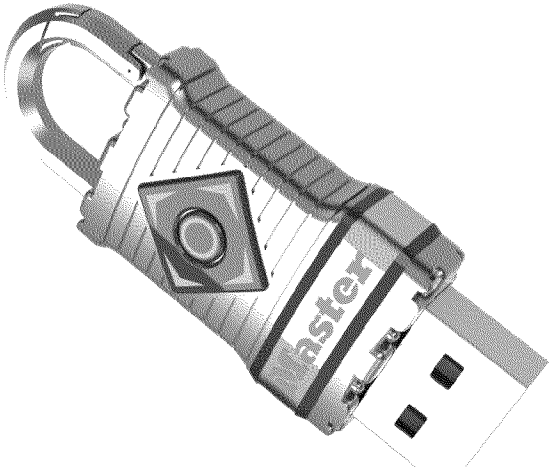


FIG. 11F



FIG. 11E



FIG. 11D

14/15

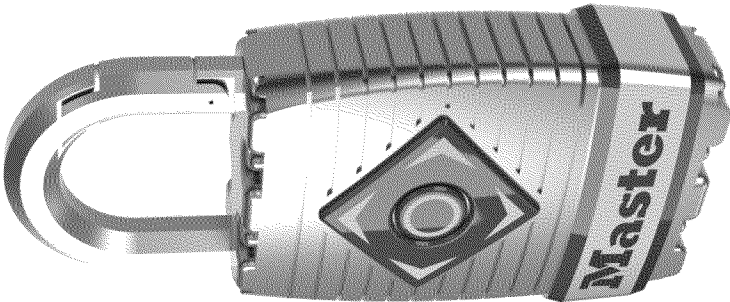


FIG. 12C

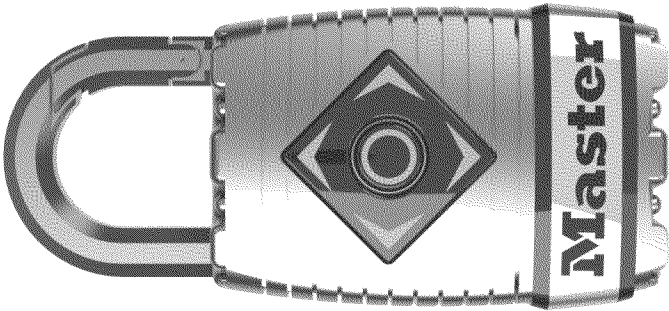


FIG. 12B



FIG. 12A

15/15

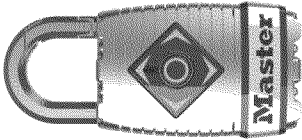


FIG. 13D

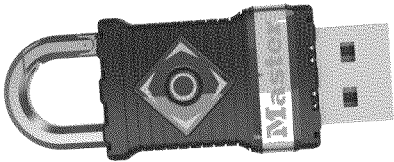


FIG. 13C

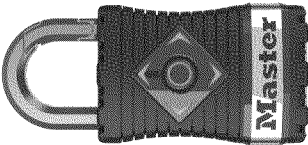


FIG. 13B

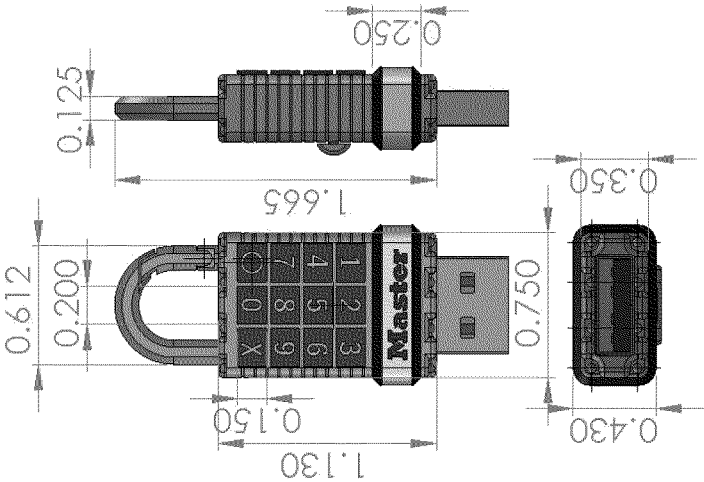


FIG. 13A

## INTERNATIONAL SEARCH REPORT

International application No.  
**PCT/US2013/026517****A. CLASSIFICATION OF SUBJECT MATTER****G06F 1/00(2006.01)i, G06F 13/14(2006.01)i, G06F 21/30(2013.01)i, G06F 21/60(2013.01)i**

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)

G06F 1/00; G06F 13/14; G06F 21/30; G06F 21/60; G06K 19/07; A63F 9/24; G06F 21/04; G06F 11/00; G06F 21/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) &amp; Keywords: portable memory(device), unlock, USB, RFID, security code, encrypt, keypad

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                | Relevant to claim No. |
|-----------|-------------------------------------------------------------------------------------------------------------------|-----------------------|
| A         | WO 2006-010952 A2 (BIZ2MOBILE LIMITED) 02 February 2006<br>See claims 10-17; and figure 2.                        | 1-30                  |
| A         | EP 2113856 A1 (TINY INDUSTRIES APS) 04 November 2009<br>See paragraphs 10-25; and figures 1-3.                    | 1-30                  |
| A         | KR 10-2006-0088578 A (JONGSUNG KIM) 07 August 2006<br>See abstract; claims 1-2; and figure 1.                     | 1-30                  |
| A         | KR 10-2011-0128424 A (MEMORETTE FM CO., LTD.) 30 November 2011<br>See paragraphs 15-33; and figures 1-2.          | 1-30                  |
| A         | WO 02-098524 A1 (WOLFE, WILLIAM, W.) 12 December 2002<br>See page 7, lines 2 - page 10, line 18; and figures 1-4. | 1-30                  |



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

"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 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

30 May 2013 (30.05.2013)

Date of mailing of the international search report

**03 June 2013 (03.06.2013)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office  
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,  
302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Byoung Sung

Telephone No. 82-42-481-8403



**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2013/026517**

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s)                                                                                                                  | Publication<br>date                                                                                          |
|-------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| WO 2006-010952 A2                         | 02.02.2006          | DE 602005012586 D1<br>EP 1771787 A2<br>EP 1771787 B1<br>GB 0416943 D0<br>GB 0701258 D0<br>GB 2430290 A<br>GB 2430290 B<br>WO 2006-010952 A3 | 19.03.2009<br>11.04.2007<br>28.01.2009<br>01.09.2004<br>28.02.2007<br>21.03.2007<br>14.01.2009<br>01.06.2006 |
| EP 2113856 A1                             | 04.11.2009          | None                                                                                                                                        |                                                                                                              |
| KR 10-2006-0088578 A                      | 07.08.2006          | None                                                                                                                                        |                                                                                                              |
| KR 10-2011-0128424 A                      | 30.11.2011          | None                                                                                                                                        |                                                                                                              |
| WO 02-098524 A1                           | 12.12.2002          | EP 1395348 A1<br>EP 1395348 A4                                                                                                              | 10.03.2004<br>14.02.2007                                                                                     |