



(22) Date de dépôt/Filing Date: 2007/05/11
(41) Mise à la disp. pub./Open to Public Insp.: 2007/11/13
(45) Date de délivrance/Issue Date: 2016/02/16
(62) Demande originale/Original Application: 2 588 309
(30) Priorité/Priority: 2006/05/13 (EP06113904.4)

(51) Cl.Int./Int.Cl. *G06F 21/62* (2013.01),
G06F 21/31 (2013.01), *G06F 21/45* (2013.01),
H04L 9/30 (2006.01)

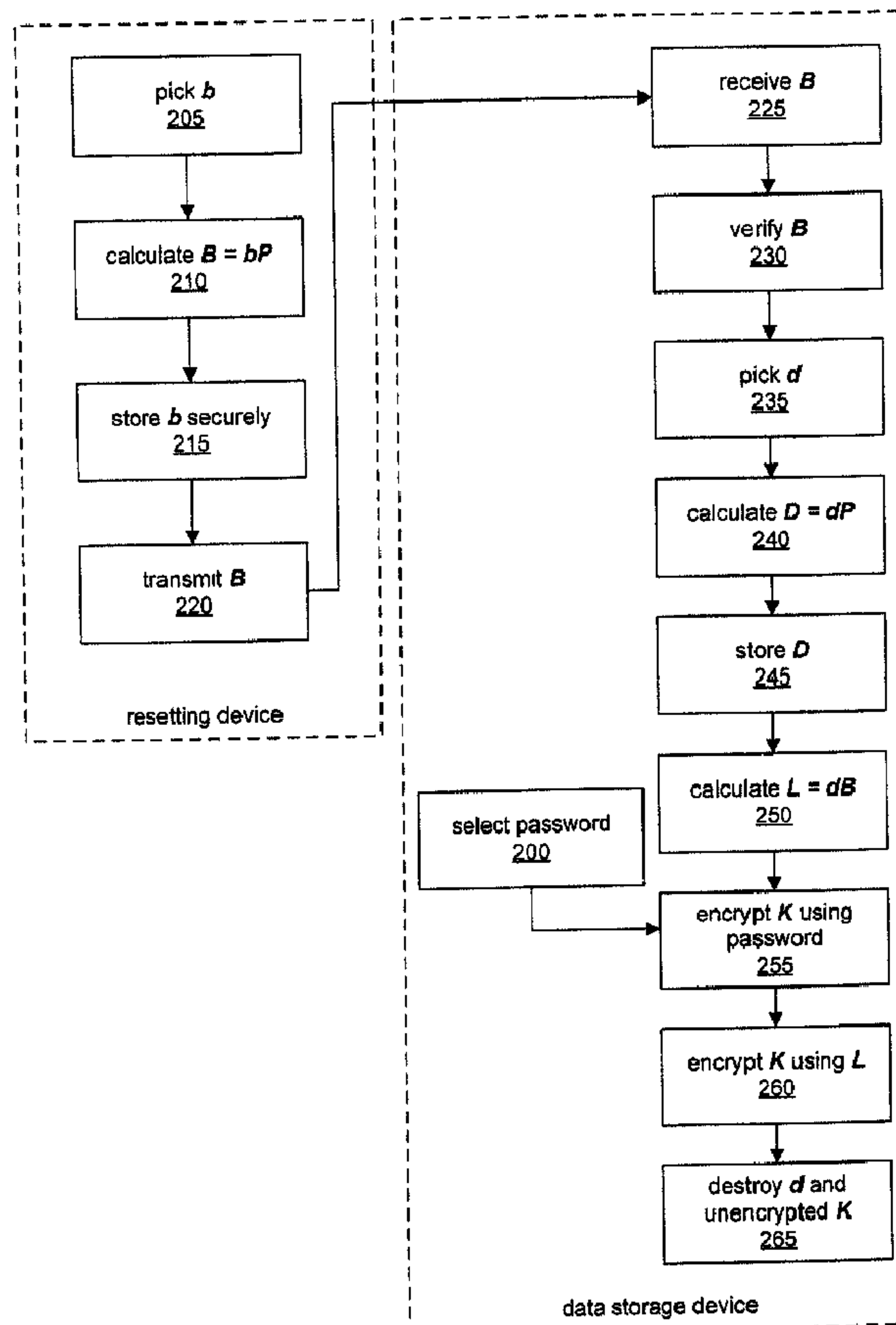
(72) Inventeurs/Inventors:
BROWN, MICHAEL S., CA;
BROWN, MICHAEL K., CA;
LITTLE, HERBERT A., CA

(73) Propriétaire/Owner:
BLACKBERRY LIMITED, CA

(74) Agent: ROWAND LLP

(54) Titre : SYSTEME ET METHODE DE REINITIALISATION A DISTANCE DE MOT DE PASSE ET DE CLE DE CHIFFREMENT

(54) Title: SYSTEM AND METHOD FOR REMOTE RESET OF PASSWORD AND ENCRYPTION KEY



(57) Abrégé/Abstract:

A method for securing data and resetting a password using a content protection key is provided, in which the content protection key itself is protected by a password. A content protection key is also protected at a data storage device with a key encryption key

(57) **Abrégé(suite)/Abstract(continued):**

generated in collaboration with an additional device such as a server. The server stores a private key required to regenerate the key encryption key, but this private key is not provided from the server to the data storage device; rather, a public key derived from the private key is provided by the server. The data storage device combines the received public key and a further private key to derive the key encryption key; the further private key itself is not stored by the data storage device, but rather its matching public key is stored. The content protection key is then encrypted using a password and the derived key encryption key. If the password is lost, data from the server and from the data storage device may be combined to recreate the key encryption key.

ABSTRACT

A method for securing data and resetting a password using a content protection key is provided, in which the content protection key itself is protected by a password. A content protection key is also protected at a data storage device with a key encryption key generated in collaboration with an additional device such as a server. The server stores a private key required to regenerate the key encryption key, but this private key is not provided from the server to the data storage device; rather, a public key derived from the private key is provided by the server. The data storage device combines the received public key and a further private key to derive the key encryption key; the further private key itself is not stored by the data storage device, but rather its matching public key is stored. The content protection key is then encrypted using a password and the derived key encryption key. If the password is lost, data from the server and from the data storage device may be combined to recreate the key encryption key.

SYSTEM AND METHOD FOR REMOTE RESET OF PASSWORD AND ENCRYPTION KEY

Reference to Prior Applications

This application is a divisional of Canadian Application No. 2,588,309, filed May 11,
5 2007, and claims priority from European Patent Office Application No. 06113904.4, filed
May 13, 2006.

Technical Field

The present disclosure relates generally to the field of computer and network security,
and in particular to password administration.

Technical Background

Data stored in the memory of a communication and/or computing device, such as a
mobile communication device, may be secured by encrypting using a content protection key.
This key, in turn, is preferably protected by, or derived in part from, a user-entered password,
PIN, or other piece of user-supplied data. This is one means to ensure that sensitive data
15 stored on the communication device is accessible only by a designated user.

Because user-entered passwords are often dependent on the user mentally recalling
the password, it is sometimes necessary for the user, an administrator or other person to reset
the user's password to another value when the user forgets the existing password. The
resetting procedure may be invoked remotely from another device in communication with the
20 user's device, for example from a server located on the same network as the user's device.
However, when content protection is enabled and data on the communication device is
encrypted using a content protection key protected by or derived from the existing user
password, the content protection key cannot be recovered without the existing user password.
If the user cannot recall the existing password, the protected data is rendered inaccessible.

25 It is therefore desirable to provide a system and method for resetting a password that
is used to protect or derive a content protection key on a device from a remote location, while
continuing to provide access to device content that is encrypted using the content protection
key.

Brief Description of the Drawings

In drawings which illustrate by way of example only a preferred embodiment of the invention,

Figure 1 is a schematic of a network for carrying out a method for remotely setting
5 and resetting a password and an encryption key.

Figure 2 is a schematic representation of a method for setting a password and an encryption key.

Figure 3 is a schematic representation of a method for resetting a password and an encryption key.

10 Figure 4 is a block diagram of a mobile communication device for use with the methods illustrated in Figures 2 and 3.

Description of Preferred Embodiments

Referring to Figure 1, an overview of an exemplary communication system for use with the embodiments described below is shown. One skilled in the art will appreciate that
15 there may be many different topologies, but the system shown in Figure 1 helps demonstrate the operation of the systems and methods described in the present application. There may be many communications devices connected to the system, that are not shown in the simple overview of Figure 1.

Figure 1 shows first communication device, here a personal computer 10, a network,
20 here the Internet 20, a server system 40, a wireless gateway 85, wireless infrastructure 90, a wireless network 105 and a second communication device, here a mobile communication device 100. It will be appreciated by those skilled in the art that the devices referred to herein as communication devices or data storage devices may comprise devices whose main function is directed to data or voice communication over a network and data storage, but may
25 also be provided with personal or productivity applications, or devices whose main function is directed to computing or executing productivity applications, but are also adapted to enable a user to communicate over a network.

A personal computer 10 may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system has an account, located within a company, possibly

connected to a local area network (LAN), and connected to the Internet 20, or connected to the Internet 20 through a large ASP (application service provider). Those skilled in the art will appreciate that the systems shown in Figure 1 may instead be connected to a wide area network (WAN) other than the Internet.

5 The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. Messages and other data may be delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network
10 105 to the mobile device 100. The particular network 105 may be any wireless network over which messages may be exchanged with a mobile communication device. The mobile device 100 may also receive data by other means, for example through a direct connection to a port provided on the mobile device 100, such as a Universal Serial Bus (USB) link.

 The server 40 may be implemented, for example, on a network computer within the
15 firewall of a corporation, a computer within an ISP or ASP system or the like. The server 40 may act as the application, network access, and/or file server for one or more communication devices. The mobile device 100, if it is configured for receiving and possibly sending e-mail, will normally be associated with an account on the server 40. The software products and other components that are often used in conjunction with the functions of the server 40
20 described herein are not shown in Figure 1, as they do not directly play a role in the system and method described below. If the server 40 acts as a message server, the server 40 may support either a so-called "pull" or "push" message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100, or the server 40 may be provided with means for automatically
25 redirecting messages addressed to the user of the mobile device 100 as they are received, respectively.

 As can be seen from the following description, the server 40 may be used to provide administrative functions for the communication devices 10 and 100, for example by establishing and transmitting information technology (IT) policies. In the preferred
30 embodiment, administrator access is provided at the server 40 for resetting device passwords,

although the system and method described herein may be implemented from another device on the network, if such administrator-level access is provided at the other device.

Data stored in a memory in the mobile device 100 or the other communication device 10, such as user- or administrator-provided content or encryption keys, may be secured in part by means of a user-entered password, PIN, or similar access control method. Content may include electronic messages, personal information, or other data caused to be entered or created by the user of the device 100 or 10. Suitable access control methods may include increasing security by providing a smart card reader for accessing security data from a smart card in the user's possession upon a request issued by the mobile device 100 or other communication device 10. Such security mechanisms prevent an unauthorized user from obtaining access to the data via the user interface provided by the device.

Preferably, a user-entered password is not the sole means by which content on the device 100 or 10 is secured. Rather, the password, using methods known in the art, is used alone or in conjunction with other encryption data to secure another key, such as a content protection key or a content protection bulk key K , that is used in turn to encrypt data. The content protection key K itself may be an Advanced Encryption Standard (AES) cryptographic key with a 128, 192, or 256 bit length, or another key for use with encryption software in accordance with another standard. As those skilled in the art will appreciate, other encryption standards may be used to define the nature of the content protection key K , although preferably a symmetric block cipher method is used. Further, the content protection key K may not be used directly to convert data into ciphertext; instead, the device 100 or 10 may be configured to use the content protection key K to generate one or more further content encryption keys for encrypting and/or decrypting data stored on the device 100 or 10. However, preferably neither the content protection key K nor any further keys derived from the key K are stored in the clear in the memory of the communication device 100 or 10.

For example, the password may be used to encrypt the content protection key K , and the encrypted content protection key K may be stored in the non-volatile memory of the device 100 or 10. The non-volatile memory is discussed below with reference to Figure 4. When the device 100 or 10 is first accessed by the user, the user is prompted to enter a password. The entered password may be compared with a password stored in the memory of

the communication device 100 or 10. Preferably, however, the password itself is not stored in the clear on the device; rather, a hash (or some other function) of the password entered by the user is compared to a hash (or some other function) of the password stored in memory. If the compared data matches, then the user is authenticated and the entered password may be
5 stored in volatile memory, also described below with reference to Figure 4, on the device 100 or 10. The password may be stored in volatile memory for the duration of a user session, which may be terminated by “logging off” the device, suspending operations of the device 100 or 10 by placing the device in a standby mode, powering off the device 100 or 10 or otherwise disconnecting a power supply from the volatile memory, or in accordance with
10 other IT policies, for example by erasing the password from volatile memory after a set period of time or immediately after user authentication.

If it is desirable to protect data stored in the memory of the device 100 or 10 using the content protection key K , when the device 100 or 10 determines that an encryption key is required for converting the data to be protected to ciphertext, it accesses the encrypted
15 content protection key K and decrypts the key using the password stored in volatile memory. The decrypted content protection key K is stored in volatile memory and is used to either encrypt the data to be protected and stored, or to generate further encryption keys for encrypting the data to be protected and stored. However the content protection key K is used, it may be deleted from volatile memory after the data is encrypted. In that case, when the
20 device 100 or 10 requires data that was previously encrypted, the device 100 or 10 again accesses the encrypted content protection key K , decrypts it and stores it in volatile memory, then either decrypts the required data by using the key K directly or by deriving the necessary further keys to decrypt the data. After the key K has been used, it is again deleted from volatile memory. The content protection key K is thus only stored in the clear in volatile
25 memory on a transitory basis. Alternatively, once the content protection key K has been decrypted a first time during a user session, it may be retained in volatile memory until the user session is terminated.

The communication device 100 or 10 may be connected to a network such as that described in Figure 1, and may be provided with IT policies relating to content protection.
30 Preferably, some security policies and features on the device 100 or 10 may be controlled

from a remote location on the network, for example from the server 40. This is particularly useful in the event that a user forgets his or her password for accessing the device 100 or 10, as an administrator or other person with sufficient privileges may force a password reset on the device 100 or 10 over the network.

5 However, if the password is used to encrypt the content protection key K , then when a password is reset the content protection key K ceases to be available to the device 100 or 10. Therefore, in accordance with the preferred embodiment, the content protection key K is re-established by the device 100 or 10 using information provided by the server 40 as follows, with reference to Figure 2.

10 When a content protection key K is established for a data storage device such as the communications device 100 or 10, the resetting device, such as the server 40, first selects or generates a private key b at step 205. The private key b is preferably generated as a random or pseudo-random number and is appropriate for use in an elliptic curve cryptography algorithm, for example in accordance with an encryption algorithm approved by the National
15 Institute of Standards and Technology (NIST). However, any alternate asymmetric key cryptography algorithm may be employed. Preferably, an elliptic curve cryptography algorithm is used, and most preferably at least a 521-bit key is used and the elliptic curve used has a cofactor of 1. Using b and a pre-determined elliptic point P , the server 40 calculates $B = bP$ at step 210 and stores b securely at step 215. b may be encrypted itself
20 using means known in the art, and stored as ciphertext. At step 220, the result B is transmitted to the communications device 100 or 10. At this point, the server 40 and the device 100 or 10 may agree to a selected encryption algorithm, or alternatively an encryption algorithm may have been previously set by the IT policies between the server 40 to the device 100 or 10.

25 The device 100 or 10 receives B at step 225 and preferably verifies that B is a valid public key at step 230, using techniques known in the art. For example, if an elliptic curve cryptography algorithm is used, then the device 100 or 10 may verify that B is a point on the pre-determined curve defined for this implementation of the algorithm. The device 100 or 10 then selects or generates a key value d at step 235. d is preferably a randomly or pseudo-
30 randomly generated value, again, preferably at least 521 bits long. The device calculates a

new public key $D = dP$ at step 240, and stores D at step 245. The device 100 or 10 also calculates a key encryption key $L = dB$ at step 250, where B is the key value received from the server 40. The content protection key K is then encrypted with the key encryption key L at step 260, and this encrypted version of K , $enc(K)_1$, is stored on the device. The content protection key K is also encrypted with the user password, and this second encrypted version of K , $enc(K)_2$, is also stored on the device. This second encryption step is indicated in Figure 2 at step 255, prior to the encryption of K by L at step 260; however, those skilled in the art will appreciate that these encryption steps may occur in reverse order. (Note that the password itself is provided to or by the device 100 or 10 at step 200, for example by the user or by some other means known in the art; the device itself may be configured to generate a password and provide the password to the user.) L and any unencrypted copies of K and d may then be destroyed by the device at step 265. Thus, the content protection key K is stored in two ciphertext forms on the device, and is preferably not stored anywhere else. The device 100 or 10 and the server 40 may also destroy B .

The steps illustrated in Figure 2 are shown in the table below:

Data Storage Device		Resetting Device
		Pick b randomly. Calculate $B = bP$. Store b securely.
Receive B .	$\leftarrow B$	Send B to data storage device.
Pick password. Verify B is a valid public key. Pick d randomly. Calculate $D = dP$. Store D . Calculate $L = dB$. Encrypt K with L . Encrypt K with password. Destroy d . Destroy K . Destroy L .		

After this procedure, the content protection key K may be recovered in one of two ways. During normal operation, the user may provide the user password in order to log in to or unlock the device, and the device may use the password to decrypt the second encrypted version of K , $enc(K)_2$, stored on the device. In the event that the password is no longer

available to decrypt the content protection key K , for example if the user cannot recall the password, a procedure such as that illustrated in Figure 3 may be followed.

When it is determined that a new password should be set for the device 100 or 10, a user or administrator at the server 40 may select or generate a new password at step 305. The server 40 then requests the public key from the device 100 or 10 at step 310. However, rather than provide the public key D in the clear, upon receipt of the request for the public key at step 415 the device 100 or 10 selects or generates a random or pseudo-random value r and temporarily stores r at step 320, and computes $D' = rD$ at step 325, preferably using elliptic curve cryptography. This blinded public key D' is transmitted to the server 40 at step 430.

After receipt of the blinded public key D' at the server 40 at step 435, the server 40 preferably verifies that D' is a valid public key at step 340, then computes a blinded key $L' = bD'$ at step 345, b having previously stored at the server 40. The server 40 then transmits this newly computed blinded key L' and the new password to the communications device 100 or 10 at step 350. The new password is preferably destroyed at the server 40 at step 390. After the device 100 or 10 receives L' at step 355, it preferably verifies that L' is a valid public key at step 360; the device 100 or 10, computes the inverse function $r^{-1}L' = L$ at step 365. The device can then use L to decrypt the first encrypted version of K , $enc(K)_1$, stored on the device at step 370.

The device 100 or 10 thus derives the original content protection key K , and may use K to decrypt any secure content stored at the device 100 or 10. After decryption, preferably the existing content protection key K is destroyed at step 375, and a new content protection key, K' , is generated at step 380 to re-encrypt the content to be secured on the device 100 or 10. This new content protection key K' is preferably protected in a manner similar to that described in relation to Figure 2; preferably, the server initiates this protection by generating a new private key b as in step 205 in Figure 2, and then proceeding with the subsequent steps to result in a new key encryption key M ; the new password, transmitted at step 350 in Figure 3, would be used in step 200 in Figure 2.

The steps illustrated in Figure 3 are shown in the table below:

Data Storage Device		Resetting Device
		Enter a new password.
	$\leftarrow$ Request Public Key	Transmit request for device public key.
Pick r randomly. Keep r in RAM. Calculate $D' = rD = rdP$.		
Send D' .	$D' \rightarrow$	Receive D' .
		Verify D' is a valid public key. Calculate $L' = bD' = brdP = rdB = rL$.
Receive L' , new password.	$\leftarrow L'$, new password	Send L' and new password.
Verify L' is a valid public key. Calculate $r^{-1}L' = r^{-1}rL = L$. Destroy r . Use L to decrypt K . Destroy K . Generate new K' . Use new password to encrypt new K' .		

- If the new content protection key K' is to be protected using a new key encryption key M , the server 40 may generate a new private key b_1 and derive a new public key B_1 from b_1 and a generating point P_1 , which may be the same generating point P as that used previously.
- 5 The remaining process to encrypt the new content protection key K' with M is described in the following table:

Data Storage Device		Resetting Device
		Pick b_1 randomly. Calculate $B_1 = b_1P_1$. Store b_1 securely.
Receive B_1 .	$\leftarrow B_1$	Send B_1 to data storage device.
Verify B_1 is a valid public key. Pick d_1 randomly. Calculate $D_1 = d_1P_1$. Store D_1 . Calculate $M = d_1B_1$. Encrypt K' with M . Encrypt K' with new password. Destroy d_1 . Destroy M .		

Thus, it will be appreciated that a means has been provided for a content protection key K to be recovered, even if the key K is encrypted by a password that is subsequently lost, by storing an alternate encrypted version of K .

In an alternate embodiment, the resetting device may immediately provide the new password selected at step 305 as part of a reset password command at step 385 without
 5 requesting the device's public key, thereby bypassing steps 310 and 315 in Figure 3. If the device is unable to immediately reset the password to the new value because content protection is enabled and K is stored only in encrypted form as determined at step 390, the device may reply with the blinded public key D' , thereby indicating to the server that the key
 10 recovery protocol should be initiated. The rest of the protocol may proceed as described as above, with the server optionally providing the new password a second time at step 350.

In a further embodiment, the key encryption key L may be used to encrypt the user password instead of encrypting the content protection K directly. In such an embodiment, both the password encrypted with L and the content protection key K encrypted with the
 15 password, or in other words $enc(K)_2$, are stored on the device. If the password is no longer available, the procedure in Figure 3 may be carried out, except that once the key encryption key L has been recovered at step 365, it may be used to first decrypt the user password, and then the user password may be used to decrypt the encrypted content protection key $enc(K)_2$.

Those skilled in the art will appreciate that the content protection key K is thus
 20 secured against a hardware-based attack. While the server 40 stores information useful for the reconstruction of the key encryption key L , a malicious user with access to the server 40 but not the device 100 or 10 will be unable to reconstruct L from the private key b alone. The reconstruction process further shields the protected content from a malicious user at the server 40, since public key D is not transmitted to the server 40; only the key D' , which is a
 25 blinded version of D , is transmitted to the server 40 such that the server 40 remains unable to compute L . It can be seen that the method of resetting a password that is used to encrypt a content protection key K , as illustrated in Figure 3, provides a means for retrieving and re-encrypting data stored on the device 100 or 10.

As another example, the systems and methods disclosed herein may be used with
 30 many different computers and devices, such as a further wireless mobile communications

device 100 shown in Figure 4. With reference to Figure 4, the user device 100 is a dual-mode mobile device and includes a transceiver 411, a microprocessor 438, a display 422, non-volatile memory 424, random access memory (RAM) 426, one or more auxiliary input/output (I/O) devices 428, a serial port 430, a keyboard 432, a speaker 434, a microphone 436, a
5 short-range wireless communications sub-system 440, and other device sub-systems 442.

The user device 100 is preferably may be a two-way communication device having voice and data communication capabilities. Thus, for example, the user device 100 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. These voice and data networks 419 may be
10 separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network.

The transceiver 411 includes a receiver 412, a transmitter 414, antennas 416 and 418, one or more local oscillators 413, and a digital signal processor (DSP) 420. The antennas 416 and 418 may be antenna elements of a multiple-element antenna, and are preferably may be
15 embedded antennas. However, the systems and methods described herein are in no way restricted to a particular type of antenna, or even to wireless communication devices. In one embodiment, the DSP 420 is used to send and receive signals to and from the antennas 416 and 418, and also provides control information to the receiver 412 and the transmitter 414. If the voice and data communications occur at a single frequency, or closely-spaced sets of
20 frequencies, then a single local oscillator 413 may be used in conjunction with the receiver 412 and the transmitter 414. Alternatively, if different frequencies are utilized for voice communications versus data communications for example, then a plurality of local oscillators 413 can be used to generate a plurality of frequencies corresponding to the voice and data networks 419. Information, which includes both voice and data information, is
25 communicated to and from the transceiver 411 via a link between the DSP 420 and the microprocessor 438.

The detailed design of the transceiver 411, such as frequency band, component selection, power level, etc., will be dependent upon the voice and data networks 419 in which the user device 100 is intended to operate. The voice and data networks 419 may be separate
30 voice networks and separate data networks, or may comprise integrated voice and data

networks. It will be appreciated by those skilled in the art that these embodiments may be implemented on a variety of voice and data networks 419, including, but not limited to, 2G, 2.5G, 3G, 4G, and other voice and data networks, such as GSM, CDMA2000, GPRS, EDGE, W-CDMA (UMTS), FOMA, EV-DO, TD-SCDMA, HSPA, HSOPA, and the like.

5 Depending upon the type of network or networks 419, the access requirements for the user device 100 may also vary. For example, in GPRS data networks, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable,
10 without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the voice and data networks 419, other than any legally required operations, such as '911' emergency calling.

 After any required network registration or activation procedures have been completed, the user device 100 may then send and receive communication signals, including
15 both voice and data signals, over the voice and networks 419. Signals received by the antenna 416 from the voice and data networks 419 are routed to the receiver 412, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation
20 and decoding to be performed using the DSP 420. In a similar manner, signals to be transmitted to the voice and data networks 419 are processed, including modulation and encoding, for example, by the DSP 420 and are then provided to the transmitter 414 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the voice and data networks 419 via the antenna 418.

25 In addition to processing the communication signals, the DSP 420 also provides for transceiver control. For example, the gain levels applied to communication signals in the receiver 412 and the transmitter 414 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 420. Other transceiver control algorithms could also be implemented in the DSP 420 in order to provide more sophisticated control of the
30 transceiver 411.

The microprocessor 438 preferably manages and controls the overall operation of the user device 100. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 420 could be used to carry out the functions of the microprocessor 438. Low-level communication functions, including at least data and voice communications, are performed through the DSP 420 in the transceiver 411. Other, high-level communication applications, such as a voice communication application 424A, and a data communication application 424B may be stored in the non-volatile memory 424 for execution by the microprocessor 438. For example, the voice communication module 424A may provide a high-level user interface operable to transmit and receive voice calls between the user device 100 and a plurality of other voice or dual-mode devices via the voice and data networks 419. Similarly, the data communication module 424B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the user device 100 and a plurality of other data devices via the voice and data networks 419. The microprocessor 438 also interacts with other device subsystems, such as the display 422, the RAM 426, the auxiliary input/output (I/O) subsystems 428, the serial port 430, the keyboard 432, the speaker 434, the microphone 436, the short-range communications subsystem 440 and any other device subsystems generally designated as 442.

Some of the subsystems shown in Figure 4 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as the keyboard 432 and the display 422 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor 438 may be stored in a persistent store such as non-volatile memory 424. The non-volatile memory 424 may be implemented, for example, as a Flash memory component, or as battery backed-up RAM. In addition to the operating system, which controls low-level functions of the mobile device 410, the non-volatile memory 424 includes a plurality of software modules 424A-424N that can be executed by the microprocessor 438 (and/or the DSP 420), including a voice

communication module 424A, a data communication module 424B, and a plurality of other operational modules 424N for carrying out a plurality of other functions. These modules are executed by the microprocessor 438 and provide a high-level interface between a user and the user device 100. This interface typically includes a graphical component provided
5 through the display 422, and an input/output component provided through the auxiliary I/O 428, keyboard 432, speaker 434, and microphone 436. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 426 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 426, before permanently writing them to a file system located
10 in a persistent store such as the Flash memory 424.

The non-volatile memory 424 may provide a file system to facilitate storage of PIM data items on the device. The PIM application may include the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 424A, 424B, via the voice and data networks 419. The PIM data items may be seamlessly
15 integrated, synchronized and updated, via the voice and data networks 419, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

Context objects representing at least partially decoded data items, as well as fully decoded data items, may be stored on the user device 100 in a volatile and non-persistent
20 store such as the RAM 426. Such information may instead be stored in the non-volatile memory 424, for example, when storage intervals are relatively short, such that the information is removed from memory soon after it is stored. However, in one embodiment, storage of this information is stored in the RAM 426 or another volatile and non-persistent store is preferred, in order to ensure that the information is erased from memory when the
25 user device 100 loses power. This prevents an unauthorized party from obtaining any stored decoded or partially decoded information by removing a memory chip from the user device 100, for example.

The user device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 430 of the user device 100 to
30 the serial port of a computer system or device. The serial port 430 may also be used to enable

a user to set preferences through an external device or software application, or to download other application modules 324N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 419.

5 A short-range communications subsystem 440 may also be included in the user device 100. The subsystem 440 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a Bluetooth® module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices.

10 The systems and methods disclosed herein are presented only by way of example and are not meant to limit the scope of the invention described herein. Other variations of the systems and methods described above will be apparent to those skilled in the art and as such are considered to be within the scope of the invention. For example, it should be understood that steps and the order of the steps in the processing described herein may be altered,
15 modified and/or augmented and still achieve the desired outcome. As only one example, the sequence of steps depicted in Figure 2 and Figure 3 may be altered with regard to the timing of the destruction of various keys and interim values, provided those keys and values were available for their intended purpose.

 The systems' and methods' data may be stored in one or more data stores. The data
20 stores can be of many different types of storage devices and programming constructs, such as RAM, ROM, Flash memory, programming data structures, programming variables, etc. It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program.

 Code adapted to provide the systems and methods described above may be provided
25 on many different types of computer-readable media including computer storage mechanisms (e.g., CD-ROM, diskette, RAM, flash memory, computer's hard drive, etc.) that contain instructions for use in execution by a processor to perform the methods' operations and implement the systems described herein.

 The computer components, software modules, functions and data structures described
30 herein may be connected directly or indirectly to each other in order to allow the flow of data

needed for their operations. It is also noted that a module or processor includes but is not limited to a unit of code that performs a software operation, and can be implemented for example as a subroutine unit of code, or as a software function unit of code, or as an object (as in an object-oriented paradigm), or as an applet, or in a computer script language, or as
5 another type of computer code.

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by any one of the patent document or patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyrights whatsoever.

CLAIMS:

1. A method for securing data in a data storage device capable of being secured by a first password, the data storage device being provided with a content protection key **K**, the method comprising:
 - receiving, at the data storage device, a public key **B** generated from a private key **b** at a remote location, the private key **b** being stored at the remote location;
 - generating, at the data storage device, a private key **d** and a public key **D** from the private key **d**;
 - generating, at the data storage device, a key encryption key **L** from the private key **d** and the public key **B**;
 - encrypting the content protection key **K** with the key encryption key **L** to provide a first encrypted content protection key, encrypting the content protection key **K** with the first password to provide a second encrypted content protection key, and storing the first and the second encrypted content protection keys in the data storage device; and
 - destroying the private key **d** and the content protection key **K** at the data storage device;
 - generating, at the data storage device, a key value **r** and a public key **D'** from the key value **r** and the public key **D**;
 - transmitting the public key **D'** to the remote location;
 - receiving, at the data storage device, a public key **L'** generated from the private key **b** and the public key **D'** at the remote location;
 - obtaining, at the data storage device, the key encryption key **L** from inverse key value r^{-1} and the public key **L'**;
 - decrypting the first encrypted content protection key using the obtained key encryption key **L** to obtain the content protection key **K**;
 - decrypting content previously encrypted using the content protection key **K** and stored in the data storage device using the content protection key **K** thus obtained;
 - encrypting the content thus decrypted using a new content protection key **K'**; and
 - encrypting the new content protection key **K'** using the key encryption key **L** to provide a new first encrypted content protection key, and encrypting the new content protection key **K'** with the first password to provide a new second encrypted content protection key.

2. The method of claim 1, further comprising, after encrypting the content protection key **K** with the key encryption key **L**, destroying the key encryption key **L**.
3. The method of claim 1 or claim 2 further comprising encrypting content stored in the data storage device using the content protection key **K** before encrypting the content protection key **K** and storing the encrypted content protection keys at the data storage device.
4. The method of claim 1 or claim 2 further comprising:
 - receiving an input password;
 - determining that the input password matches the first password;
 - decrypting the second encrypted content protection key using the input password to obtain the content protection key **K**; and
 - using the content protection key **K** obtained by decrypting the second encrypted content protection key to encrypt content for storage in the data storage device.
5. The method of claim 4 further comprising using the content protection key **K** obtained by decrypting the second encrypted content protection key to decrypt encrypted content stored in the data storage device.
6. The method of claim 1, further comprising:
 - providing a new key protection key **M**;
 - receiving a second password; and
 - encrypting the content protection key **K** using the new key encryption key **M** to provide a new first encrypted content protection key, and encrypting the content protection key **K** with the second password to provide a new second encrypted content protection key.
7. The method of claim 6 wherein providing the new key protection key **M** comprises:
 - receiving, at the data storage device, a public key **B₁** generated from a private key **b₁** at the remote location, the private key **b₁** being stored at the remote location;

generating, at the data storage device, a private key $\mathbf{d}_1$ and a public key $\mathbf{D}_1$ from the private key $\mathbf{d}_1$;

generating, at the data storage device, a key encryption key $\mathbf{M}$ from the private key $\mathbf{d}_1$ and the public key $\mathbf{B}_1$; and

destroying, at the data storage device, the private key $\mathbf{d}_1$ and the content protection key $\mathbf{K}$ while retaining the new first and the new second encrypted content protection keys.

8. The method of either claim 6 or 7 further comprising, after encrypting the content protection key $\mathbf{K}$ with the new key encryption key $\mathbf{M}$, destroying the new key encryption key $\mathbf{M}$.

9. The method of any one of claims 6 to 8, further comprising receiving, at the data storage device, a request for a public key from the remote location, prior to generating the key value $\mathbf{r}$ and the public key $\mathbf{D}'$.

10. The method of any one of claims 6 to 8, further comprising receiving, at the data storage device, a reset password command from the remote location, prior to generating the key value $\mathbf{r}$ and the public key $\mathbf{D}'$.

11. The method of claim 1, further comprising:

decrypting content previously encrypted using the content protection key $\mathbf{K}$ and stored in the data storage device using the content protection key $\mathbf{K}$ thus obtained;

providing a new content protection key $\mathbf{K}'$;

encrypting the content thus decrypted using the new content protection key $\mathbf{K}'$;

providing a new key encryption key $\mathbf{M}$; and

encrypting the new content protection key $\mathbf{K}'$ using the password to provide a new first encrypted content protection key, and encrypting the new content protection key $\mathbf{K}'$ with the new key encryption key $\mathbf{M}$ to provide a new second encrypted content protection key.

12. The method of claim 11 wherein providing the new key protection key $\mathbf{M}$ comprises:

receiving, at the data storage device, a public key B_1 generated from a private key b_1 at a remote location, the private key b_1 being stored at the remote location;

generating, at the data storage device, a private key d_1 and a public key D_1 from the private key d_1 ;

generating, at the data storage device, the key encryption key M from the private key d_1 and the public key B_1 ; and

destroying, at the data storage device, the private key d_1 and the new content protection key K' while retaining the new first and the new second encrypted content protection keys.

13. The method of either claim 11 or 12 further comprising, after encrypting the new content protection key K' with the new key encryption key M , destroying the new key encryption key M .

14. The method of either claim 7 or 12 wherein the public key B is also generated from a generating point P , and the public key B_1 is also generated from a generating point P_1 .

15. A method for securing data in a data storage device capable of being secured by a first password, the data storage device being provided with a content encryption key K , the method comprising:

receiving, at the data storage device, a public key B generated from a private key b at a remote location, the private key b being stored at the remote location;

generating, at the data storage device, a private key d and a public key D from the private key d ;

generating, at the data storage device, a key encryption key L from the private key d and the public key B ;

encrypting the content encryption key K with the first password to provide an encrypted content protection key, and storing the encrypted content protection key in the data storage device;

encrypting the first password with the key encryption key L to provide a first encrypted password, and storing the encrypted password in the data storage device;

destroying the private key **d** and the unencrypted content encryption key **K** at the data storage device;

generating, at the data storage device, a key value **r** and a public key **D'** from the key value **r** and the public key **D**;

transmitting the public key **D'** to the remote location;

receiving, at the data storage device, a public key **L'** generated from the private key **b** and the public key **D'** at the remote location;

obtaining, at the data storage device, the key encryption key **L** from the inverse key value r^{-1} and **L'**;

decrypting the first encrypted password using **L** to obtain the first password;

decrypting the encrypted content protection key using the first password obtained by decrypting the first encrypted password to obtain the content protection key **K**;

decrypting content previously encrypted using the content protection key **K** and stored in the data storage device using the content protection key **K** thus obtained;

encrypting the content thus decrypted using a new content protection key **K'**; and

encrypting the new content protection key **K'** using the first password to provide a new encrypted content protection key.

16. The method of claim 15 further comprising, after encrypting the first password with the key encryption key **L**, destroying the key encryption key **L**.

17. The method of either claim 15 or 16 further comprising encrypting content stored in the data storage device using the content protection key **K** before encrypting the content protection key **K** and storing the encrypted content protection key at the data storage device.

18. The method of claim 17 further comprising:

receiving an input password;

determining that the input password matches the first password, and if the input password matches the first password,

decrypting the encrypted content protection key using the input password to obtain the content protection key **K**; and

using the content protection key **K** obtained by decrypting the encrypted content protection key using the input password to encrypt content for storage in the data storage device.

19. The method of claim 18 further comprising using the content protection key **K** obtained by decrypting the encrypted content protection key using the input password to decrypt encrypted content stored in the data storage device.

20. The method of claim 15, further comprising:

providing a new key protection key **M**;

receiving a second password; and

encrypting the content protection key **K** using the second password to provide a new encrypted content protection key, and encrypting the second password using the new key encryption key **M** to provide a second encrypted password.

21. The method of claim 20 wherein providing a new key protection key **M** comprises:

receiving, at a data storage device, a public key **B₁** generated from a private key **b₁** at a remote location, the private key **b₁** being stored at the remote location;

generating, at the data storage device, a private key **d₁** and a public key **D₁** from the private key **d₁**;

generating, at the data storage device, a key encryption key **M** from the private key **d₁** and the public key **B₁**; and

destroying the private key **d₁** and the content protection key **K** at the data storage device after providing the new encrypted content protection key.

22. The method of either claim 20 or 21 further comprising, after encrypting the second password using the new key encryption key **M**, destroying the new key encryption key **M**.

23. The method of any one of claims 15 to 22, further comprising receiving, at the data storage device, a request for a public key from the remote location, prior to generating the key value **r** and the public key **D'**.
24. The method of any one of claims 15 to 22, further comprising receiving, at the data storage device, a reset password command from the remote location, prior to generating the key value **r** and the public key **D'**.
25. The method of claim 15, further comprising:
 decrypting content previously encrypted using the content protection key **K** and stored in the data storage device using the content protection key **K** thus obtained;
 providing a new content protection key **K'**;
 encrypting the content thus decrypted using the new content protection key **K'**;
 providing a new key encryption key **M**; and
 encrypting the new content protection key **K'** using the password to provide a new encrypted content protection key, and encrypting the first password with the new key encryption key **M** to provide a new first encrypted password.
26. The method of claim 25 wherein providing the new key encryption key **M** comprises:
 receiving, at a data storage device, a public key **B₁** generated from a private key **b₁** at a remote location, the private key **b₁** being stored at the remote location;
 generating, at the data storage device, a private key **d₁** and a public key **D₁** from the private key **d₁**;
 generating, at the data storage device, a key encryption key **M** from the private key **d₁** and the public key **B₁**; and
 destroying the private key **d₁** and the new content protection key **K'** at the data storage device after providing the new encrypted content protection key.
27. The method of either claim 25 or 26, further comprising, after encrypting the first password with the new key encryption key **M**, destroying the new key encryption key **M**.

28. The method of either claim 21 or 26 wherein the public key **B** is also generated from a generating point **P**, and the public key **B₁** is also generated from a generating point **P₁**.
29. The method of claim 14 or claim 28 wherein the generating point **P₁** is the same as the generating point **P**.
30. A computing device adapted to carry out the method of any one of claims 1 to 14 or 15 to 29.
31. The computing device of claim 30, wherein the computing device is a mobile communication device.
32. An electronic device-readable medium having recorded thereon electronic device-executable instructions that when executed by an electronic device cause the electronic device to implement the method of any one of claims 1 to 14 or 15 to 29.
33. A device, comprising:
- at least one memory component for storing data, at least one password, and keys; and
 - at least one processor configured to:
 - enable receipt of a public key $\mathbf{B} = \mathbf{bP}$ from a remote location, wherein **P** is an elliptic curve point and **b** is a private key stored at the remote location;
 - compute and store a public key $\mathbf{D} = \mathbf{dP}$ in the at least one memory component, wherein **d** is a random value generated at the device for computing the public key **D** and then deleted once the public key **D** is computed;

encrypt a content protection key **K** for storage by encrypting the content protection key **K** using a key encryption key $L = dB$, and storing the content protection key **K** thus encrypted in the at least one memory component;

delete any unencrypted copies of the content protection key **K**;

recover the content protection key **K** without using the password by:

generating a random value **r**;

computing a public key $D' = rD$;

transmitting the public key **D'** to the remote location;

receiving from the remote location a public key $L' = bD'$;

computing $r^{-1}L'$ to derive the key encryption key **L**; and

decrypting, using the key encryption key **L** thus derived, the content protection key **K** previously encrypted using **L**;

decrypt content previously encrypted using the content protection key **K** using the content protection key **K** thus recovered;

encrypt the decrypted content using a new content protection key **K'**; and

protect the new content protection key **K'** by encryption.

34. The device of claim 33, wherein the at least one processor is further configured to encrypt and decrypt data with the content protection key **K**.

35. The device of claim 33, wherein the at least one processor is further configured to use the content protection key **K** to generate one or more further content protection keys for encrypting and decrypting data.

36. The device of claim 33, wherein the at least one processor is further configured to encrypt the content protection key **K** using a password, and store the content protection key **K** thus encrypted in the at least one memory component.
37. The device of claim 36, wherein the at least one processor is further configured to:
- enable receipt of the password as input;
- in response to receipt of the password, decrypt the content protection key **K** encrypted using the password; and
- decrypt content previously encrypted using the content protection key **K** thus decrypted.
38. The device of claim 33, wherein the at least one processor is further configured to protect the new content protection key **K'** by encryption using the key encryption key **L**.
39. The device of claim 33, wherein the at least one processor is further configured to protect the new content protection key **K'** by encryption using a new key encryption key **M**.
40. The device of claim 33, wherein the at least one processor is further configured to protect the new content protection key **K'** by encryption using a new password.
41. The device of claim 40, wherein the at least one processor is further configured to protect the new content protection key **K'** by encryption using a new key encryption key **M**.
42. The device of claim 33, wherein the at least one memory component comprises:
- volatile memory for storing unencrypted data, passwords, and keys; and
- non-volatile memory for storing encrypted data and encrypted keys.
43. The device of claim 33, wherein the device is a mobile communication device.
44. The device of claim 33, wherein the device is a personal computer.
45. A device, comprising:

at least one memory component for storing data, at least one password, and keys;

at least one processor configured to:

enable receipt of a public key $\mathbf{B} = \mathbf{bP}$ from a remote location, wherein $\mathbf{P}$ is an elliptic curve point and $\mathbf{b}$ is a private key stored at the remote location;

compute and store a public key $\mathbf{D} = \mathbf{dP}$ in the at least one memory component, wherein $\mathbf{d}$ is a random value generated at the device for computing the public key $\mathbf{D}$ and then deleted once the public key $\mathbf{D}$ is computed;

encrypt a content protection key $\mathbf{K}$ for storage by:

encrypting the content protection key $\mathbf{K}$ using a password, and storing the content protection key $\mathbf{K}$ thus encrypted in the at least one memory component;
and

encrypting the password using a key encryption key $\mathbf{L} = \mathbf{dB}$, and storing the password thus encrypted in the at least one memory component;

delete any unencrypted copies of the content protection key $\mathbf{K}$;

recover the password from the encrypted password stored in the at least one memory component by:

generating a random value $\mathbf{r}$;

computing a public key $\mathbf{D}' = \mathbf{rD}$;

transmitting the public key $\mathbf{D}'$ to the remote location;

receiving from the remote location a public key $\mathbf{L}' = \mathbf{bD}'$;

computing $\mathbf{r}^{-1}\mathbf{L}'$ to derive the key encryption key $\mathbf{L}$; and

decrypting, using the key encryption key **L** thus derived, the password previously encrypted using **L**;

decrypt the encrypted content protection key **K** using the password thus recovered;

decrypt content previously encrypted using the content protection key **K** using the content protection key **K** thus decrypted;

encrypt the decrypted content using a new content protection key **K'**; and

protect the new content protection key **K'** by encryption.

46. The device of claim 45, wherein the at least one processor is further configured to encrypt and decrypt data with the content protection key **K**.

47. The device of claim 45, wherein the at least one processor is further configured to use the content protection key **K** to generate one or more further content protection keys for encrypting and decrypting data.

48. The device of claim 45, wherein the at least one processor is further configured to protect the new content protection key **K'** by encryption using a new password.

49. The device of claim 45, wherein the at least one processor is further configured to encrypt the new password using a new key encryption key **M**.

50. The device of claim 45, wherein the at least one memory component comprises:

volatile memory for storing unencrypted data, passwords, and keys; and

non-volatile memory for storing encrypted data and encrypted keys.

51. The device of claim 45, wherein the device is a mobile communication device.

52. The device of claim 45, wherein the device is a personal computer.

53. An electronic device-readable medium having recorded thereon electronic device-executable instructions that when executed by an electronic device cause the electronic device to implement the method of:

receiving a public key $\mathbf{B} = \mathbf{bP}$ from a remote entity, wherein $\mathbf{P}$ is an elliptic curve point and $\mathbf{b}$ is a private key;

computing, at the electronic device, a public key $\mathbf{D} = \mathbf{dP}$, wherein $\mathbf{d}$ is a random value generated at the electronic device, and storing $\mathbf{D}$;

computing a key encryption key $\mathbf{L} = \mathbf{dB}$;

encrypting a content encryption key $\mathbf{K}$ using the key encryption key $\mathbf{L}$ to provide a first encrypted content encryption key, and storing the first encrypted content encryption key at the electronic device;

subsequently recovering the content encryption key $\mathbf{K}$ from the first encrypted content encryption key at the electronic device by:

generating a random value $\mathbf{r}$ and computing a public key $\mathbf{D}' = \mathbf{rD}$;

transmitting the public key $\mathbf{D}'$ to the remote entity and receiving in response a public key $\mathbf{L}' = \mathbf{bD}'$; and

decrypting the first encrypted content protection key using a value for the key encryption key $\mathbf{L}$ calculated as $\mathbf{r}^{-1}\mathbf{L}'$, wherein $\mathbf{r}^{-1}$ is an inverse value of $\mathbf{r}$.

54. The electronic device-readable medium of claim 53, wherein the method further comprises:

further encrypting the content encryption key $\mathbf{K}$ using a password to provide a second encrypted content encryption key, and storing the second encrypted content encryption key at the electronic device; and

while the password is retained in volatile memory of the electronic device, using the password to decrypt the second encrypted content encryption key to obtain the content encryption key **K** for use in encrypting and decrypting data at the electronic device.

55. The electronic device-readable medium of claim 54, wherein the method further comprises receiving a new password, generating a new content encryption key **K'**, and:

decrypting any data encrypted using the recovered content encryption key **K**;

encrypting the data thus decrypted using the new content encryption key **K'**; and

encrypting the new content encryption key **K'**.

56. The electronic device-readable medium of claim 55, wherein the new content encryption key **K'** is encrypted using the key encryption key **L**.

57. The electronic device-readable medium of claim 55, wherein the new content encryption key **K'** is encrypted using a new key encryption key **M**.

58. The electronic device-readable medium of claim 57, wherein the method further comprises:

receiving a new public key $\mathbf{B}_1 = \mathbf{b}_1\mathbf{P}_1$ from the remote entity, wherein $\mathbf{P}_1$ is an elliptic curve point and $\mathbf{b}_1$ is a private key;

computing, at the electronic device, a new public key $\mathbf{D}_1 = \mathbf{d}_1\mathbf{P}_1$, wherein $\mathbf{d}_1$ is a random value generated at the electronic device, and storing $\mathbf{D}_1$; and

computing the new key encryption key $\mathbf{M} = \mathbf{d}_1\mathbf{B}_1$.

59. The electronic device-readable medium of claim 53, wherein encrypting the content encryption key **K** using the key encryption key **L** is carried out using an encryption method other than elliptic curve cryptography.

60. The electronic device-readable medium of claim 54, wherein encrypting the content encryption key **K** using the password is carried out using an encryption method other than elliptic curve cryptography.

61. The electronic device-readable medium of claim 54, wherein any data encrypted using the content encryption key **K** is encrypted using a key derived from the content encryption key **K**.

62. An electronic device-readable medium having recorded thereon electronic device-executable instructions that when executed by an electronic device cause the electronic device to implement the method of:

receiving a public key $\mathbf{B} = \mathbf{bP}$ from a remote entity, wherein **P** is an elliptic curve point and **b** is a private key;

computing, at the electronic device, a public key $\mathbf{D} = \mathbf{dP}$, wherein **d** is a random value generated at the electronic device, and storing **D**;

encrypting a password using a key encryption key $\mathbf{L} = \mathbf{dB}$ to provide an encrypted password, and storing the encrypted password at the electronic device;

subsequently recovering the password from the encrypted password at the electronic device by:

generating a random value **r** and computing a public key $\mathbf{D}' = \mathbf{rD}$;

transmitting the public key **D'** to the remote entity and receiving in response a public key $\mathbf{L}' = \mathbf{bD}'$; and

decrypting the encrypted password using a value for the key encryption key **L** calculated as $\mathbf{r}^{-1}\mathbf{L}'$, wherein $\mathbf{r}^{-1}$ is an inverse value of **r**.

63. The electronic device-readable medium of claim 62, wherein the method further comprises:

using the password to encrypt a content protection key **K** to provide an encrypted content protection key, the content protection key **K** being used to encrypt and decrypt data stored at the electronic device.

64. The electronic device-readable medium of claim 63, wherein the method further comprises receiving a new password, generating a new content encryption key **K'**, and:

decrypting, using the password thus recovered, the encrypted content protection key;

decrypting any data encrypted using the content encryption key **K** obtained by decrypting the encrypted content protection key;

encrypting the data thus decrypted using the new content encryption key **K'**; and

encrypting the new content encryption key **K'**.

65. The electronic device-readable medium of claim 64, wherein the new content encryption key **K'** is encrypted using the key encryption key **L**.

66. The electronic device-readable medium of claim 64, wherein the new content encryption key **K'** is encrypted using a new key encryption key **M**.

67. The electronic device-readable medium of claim 66, wherein the method further comprises:

receiving a new public key $\mathbf{B}_1 = \mathbf{b}_1\mathbf{P}_1$ from the remote entity, wherein $\mathbf{P}_1$ is an elliptic curve point and $\mathbf{b}_1$ is a private key;

computing, at the electronic device, a new public key $\mathbf{D}_1 = \mathbf{d}_1\mathbf{P}_1$, wherein $\mathbf{d}_1$ is a random value generated at the electronic device, and storing $\mathbf{D}_1$; and

computing the new key encryption key $\mathbf{M} = \mathbf{d}_1\mathbf{B}_1$.

68. The electronic device-readable medium of claim 62, wherein encrypting the password using the key encryption key **L** is carried out using an encryption method other than elliptic curve cryptography.

69. The electronic device-readable medium of claim 63, wherein encrypting the content encryption key **K** using the password is carried out using an encryption method other than elliptic curve cryptography.

70. An electronic device-readable medium having recorded thereon electronic device-executable instructions that when executed by an electronic device cause the electronic device to implement the method of:

receiving an instruction to reset a password at the electronic device, wherein the password is used at the electronic device to encrypt and decrypt a content encryption key **K**, the content encryption key **K** also being encrypted using a key encryption key $\mathbf{L} = \mathbf{dB}$, wherein **d** is a random value generated at the electronic device and **B** is a public key provided by a remote entity;

determining that the content encryption key **K** is not available in decrypted form;

transmitting a public key $\mathbf{D}' = \mathbf{rD}$ to a remote entity and receiving in response a public key $\mathbf{L}' = \mathbf{bD}'$, wherein **r** is a random value generated at the electronic device, **D** is a public key equal to $\mathbf{dP}$, wherein **P** is an elliptic curve point and **b** is a private key held by the remote entity, wherein $\mathbf{B} = \mathbf{bP}$;

computing $\mathbf{r}^{-1}\mathbf{L}'$, wherein $\mathbf{r}^{-1}$ is an inverse value of **r**; and

decrypting the content encryption key **K** encrypted by the key encryption key **L** using the computed $\mathbf{r}^{-1}\mathbf{L}$.

71. The electronic device-readable medium of claim 70, further comprising, after decrypting the content encryption key **K** encrypted by the key encrypted key **L** using the computed $\mathbf{r}^{-1}\mathbf{L}$:

decrypting any data encrypted using the content encryption key **K**;

re-encrypting the data thus decrypted using a new content encryption key $\mathbf{K}'$; and

encrypting the new content encryption key $\mathbf{K}'$ using each of the computed $\mathbf{r}^{-1}\mathbf{L}$ and a new password.

72. The electronic device-readable medium of claim 70, further comprising, after decrypting the content encryption key $\mathbf{K}$ encrypted by the key encrypted key $\mathbf{L}$ using the computed $\mathbf{r}^{-1}\mathbf{L}$:

decrypting any data encrypted using the content encryption key $\mathbf{K}$;

re-encrypting the data thus decrypted using a new content encryption key $\mathbf{K}'$; and

encrypting the new content encryption key $\mathbf{K}'$ using a new password; and

encrypting the new password using the computed $\mathbf{r}^{-1}\mathbf{L}$.

1/4

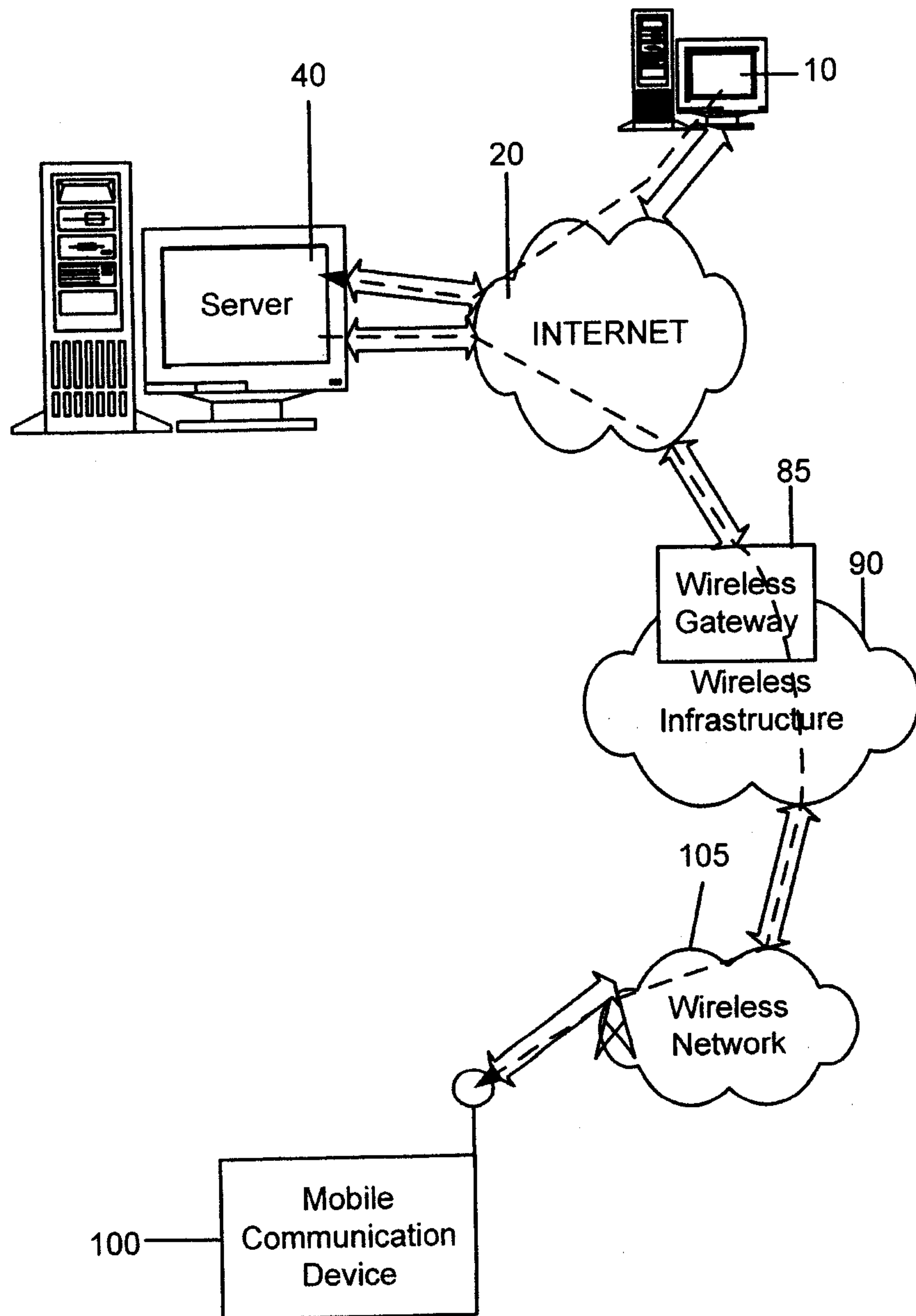


Figure 1

2/4

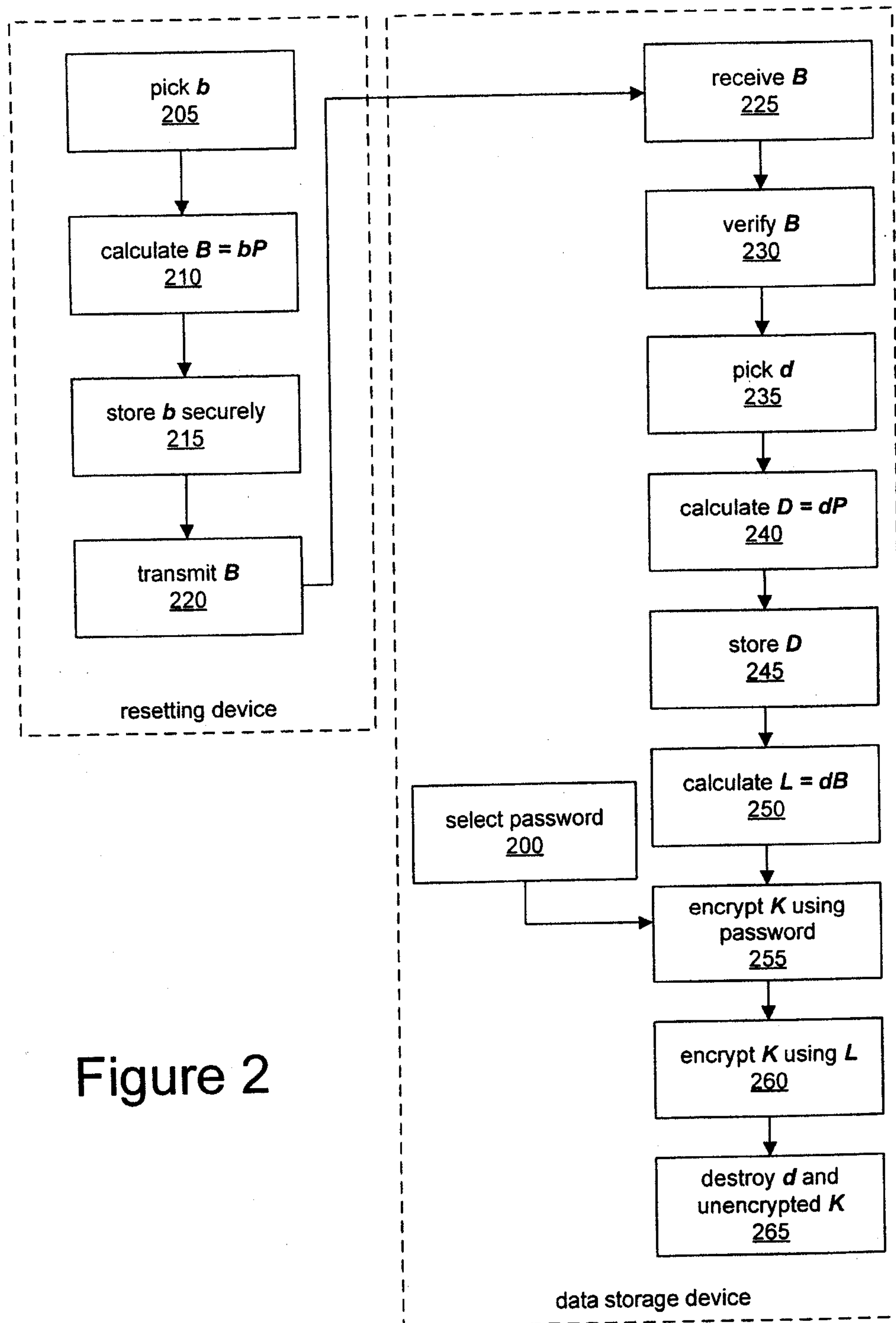
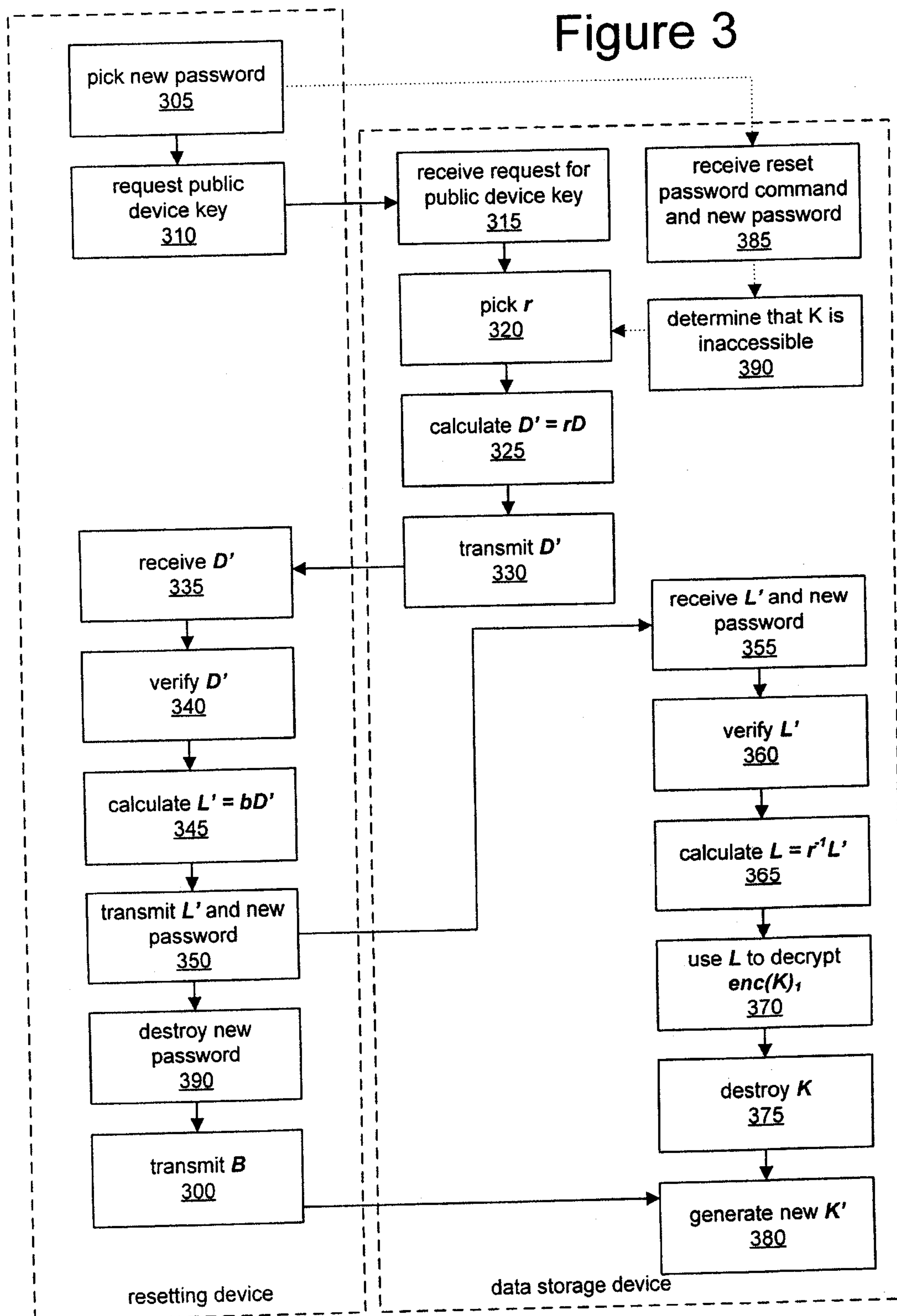


Figure 2

3/4

Figure 3



4/4

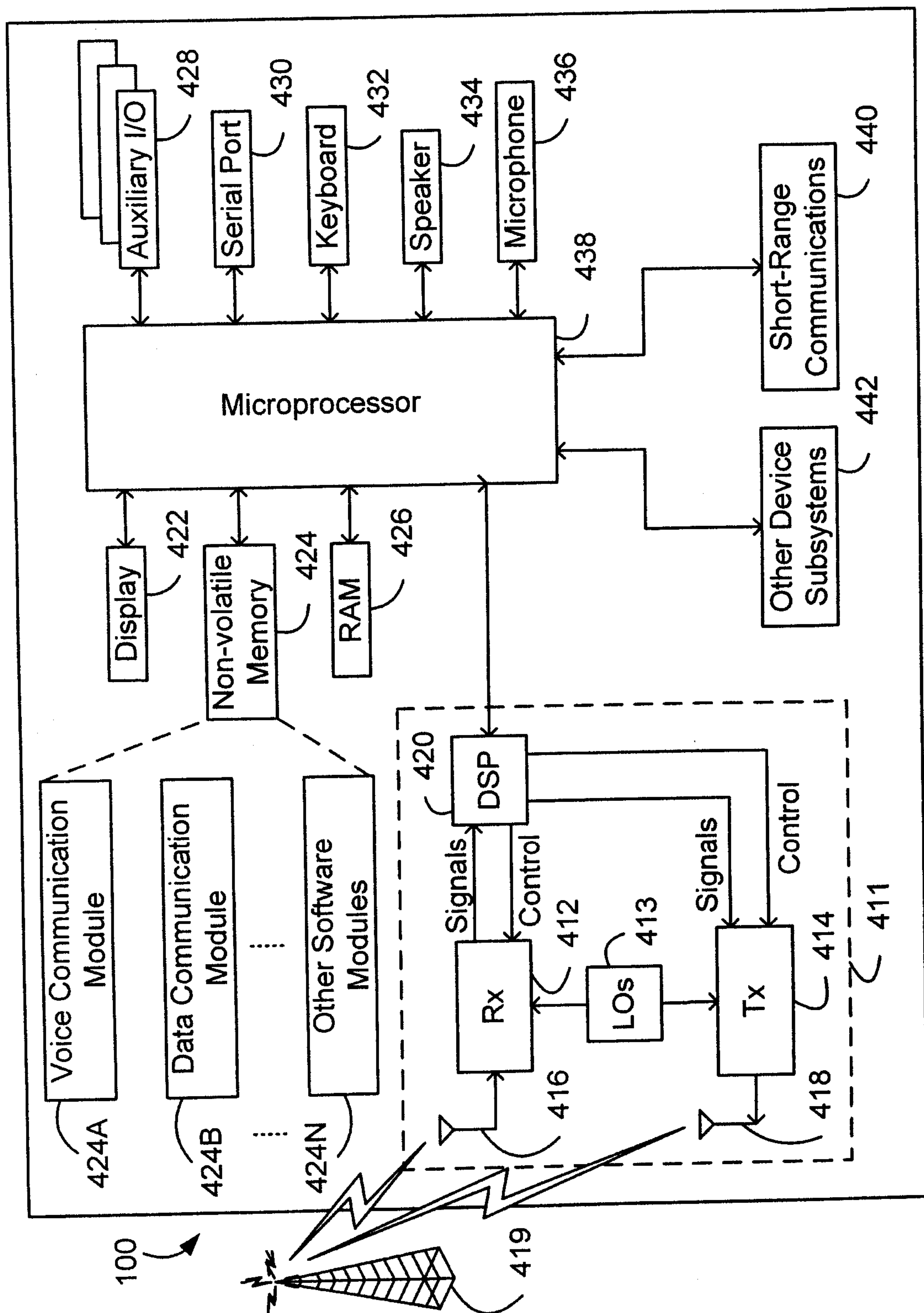


Figure 4

pick b
205

calculate $B = bP$
210

store b securely
215

transmit B
220

resetting device

receive B
225

verify B
230

pick d
235

calculate $D = dP$
240

store D
245

calculate $L = dB$
250

encrypt K using
password
255

encrypt K using L
260

destroy d and
unencrypted K
265

select password
200

data storage device