(12) UK Patent (19) GB (11) 2580549 (13) B

(45) Date of B Publication 23.12.2020

(54) Title of the Invention: Data security system with encryption

(51) INT CL: ***H04L 29/06*** (2006.01) ***G06F 21/35*** (2013.01) ***G06F 21/60*** (2013.01) ***H04L 9/32*** (2006.01)

(21) Application No: **1919421.6**

(22) Date of Filing: **03.01.2017**

Date Lodged: **30.12.2019**

(30) Priority Data:
(31) **14987749** (32) **04.01.2016** (33) **US**

(62) Divided from Application No
1811137.7 under section 15(9) of the Patents Act 1977

(43) Date of A Publication **22.07.2020**

(56) Documents Cited:
WO 2009/042820 A1
WO 2008/156848 A1
US 20100174922 A1
US 20080303631 A1
US 20080098134 A1
US 20030109218 A1
US 20030093693 A1

(58) Field of Search:
As for published application 2580549 A viz:
INT CL **G06F, G11B, H04L, H04W**
Other: **WPI**, **EPODOC**, **XPI3E**
updated as appropriate

Additional Fields
Other: **None**

(72) Inventor(s):
Lev M Bolotin
Marc Singer
Alex Lemelev

(73) Proprietor(s):
Clevx, LLC
9306 NE, 125th Street, Kirkland, Washington 98034, United States of America

(74) Agent and/or Address for Service:
Schwegman Lundberg Woessner Limited
Hillington Park Innovation Centre, 1 Ainslie Road, GLASGOW, G52 4RU, United Kingdom

GB 2580549 B

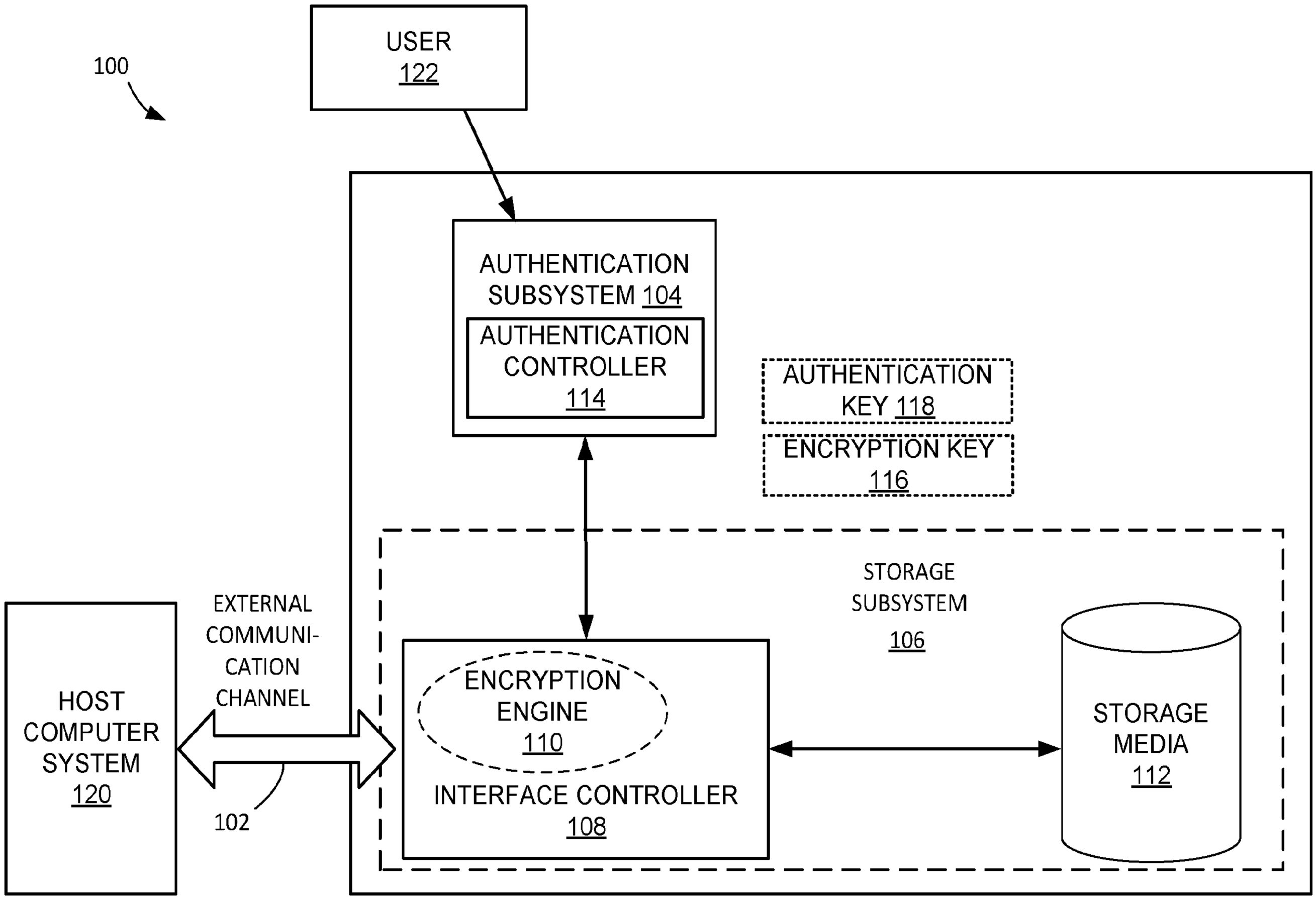

100
USER
122
AUTHENTICATION
SUBSYSTEM 104
AUTHENTICATION
CONTROLLER
114
AUTHENTICATION
KEY 118
ENCRYPTION KEY
116
STORAGE
SUBSYSTEM
106
EXTERNAL
COMMUNI-
CATION
CHANNEL
HOST
COMPUTER
SYSTEM
120
ENCRYPTION
ENGINE
110
INTERFACE CONTROLLER
108
STORAGE
MEDIA
112
102

FIG. 1

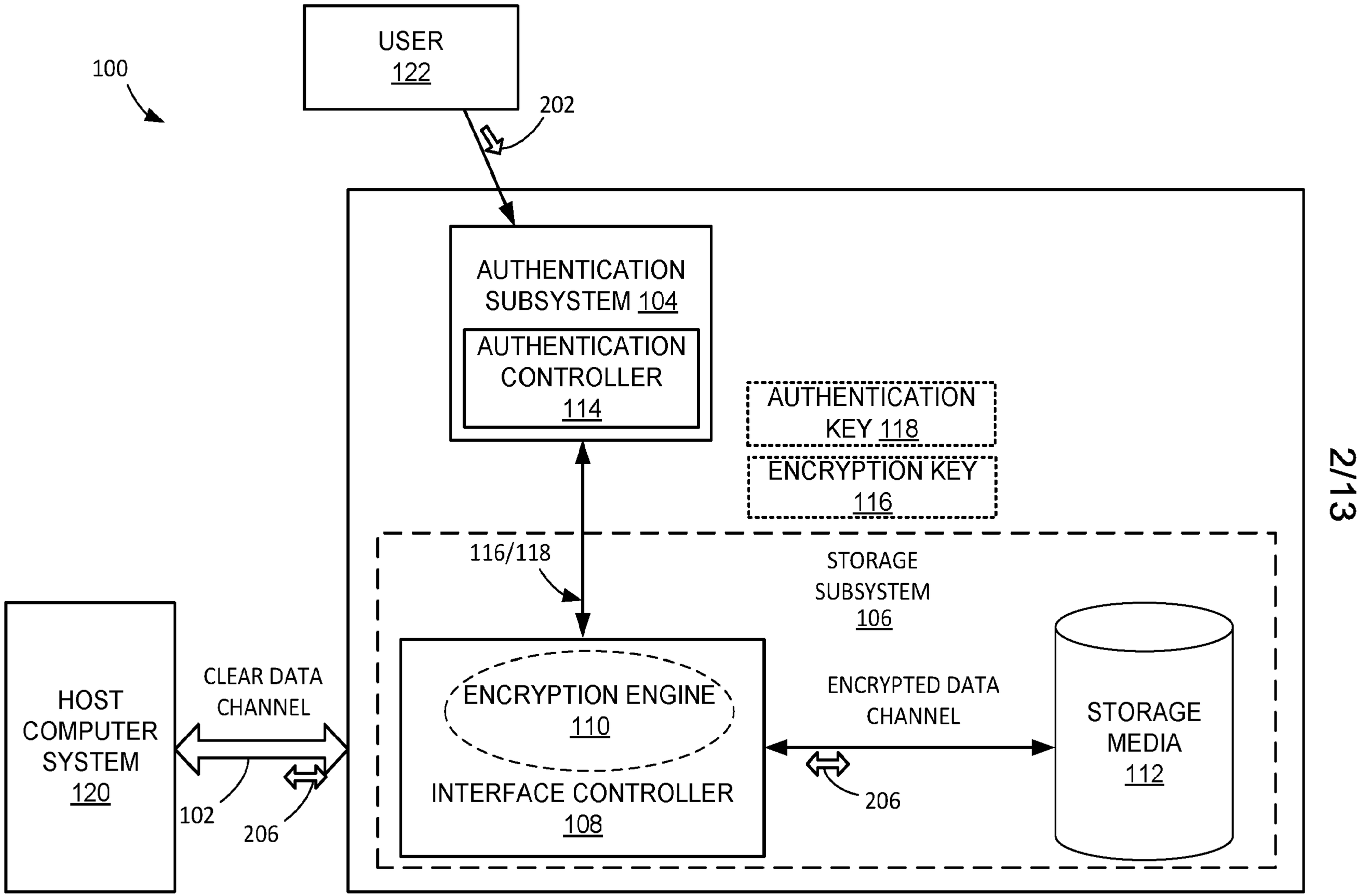

100
USER
122
202
AUTHENTICATION
SUBSYSTEM 104
AUTHENTICATION
CONTROLLER
114
AUTHENTICATION
KEY 118
ENCRYPTION KEY
116
116/118
STORAGE
SUBSYSTEM
106
HOST
COMPUTER
SYSTEM
120
CLEAR DATA
CHANNEL
102
206
ENCRYPTION ENGINE
110
INTERFACE CONTROLLER
108
ENCRYPTED DATA
CHANNEL
206
STORAGE
MEDIA
112

FIG. 2

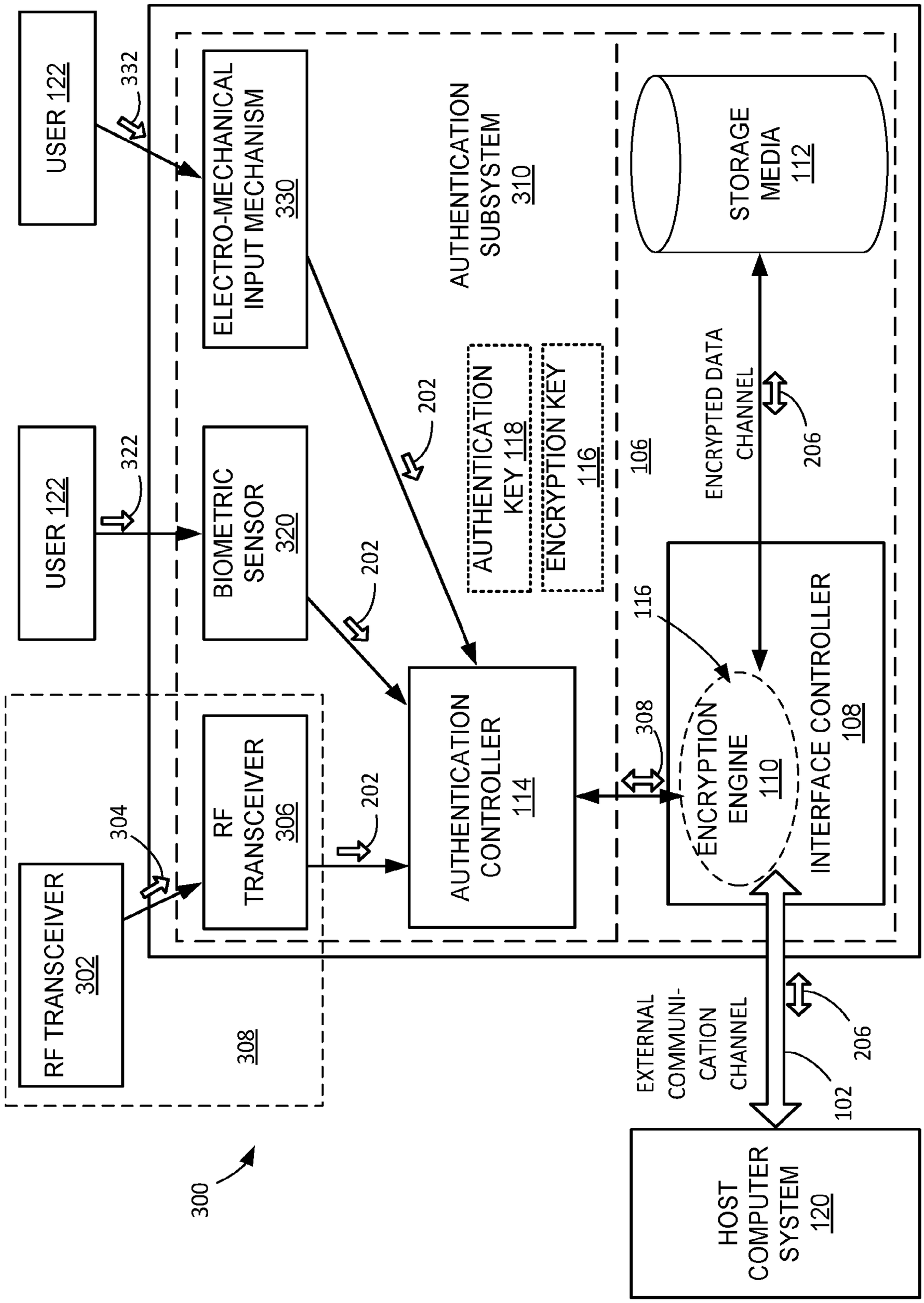

USER 122
322
BIOMETRIC SENSOR 320
332
ELECTRO-MECHANICAL INPUT MECHANISM 330
202
AUTHENTICATION SUBSYSTEM 310
AUTHENTICATION KEY 118
ENCRYPTION KEY 116
106
STORAGE MEDIA 112
ENCRYPTED DATA CHANNEL
206
116
RF TRANSCEIVER 302
304
RF TRANSCEIVER 306
AUTHENTICATION CONTROLLER 114
308
ENCRYPTION ENGINE 110
INTERFACE CONTROLLER 108
EXTERNAL COMMUNI-CATION CHANNEL
102
HOST COMPUTER SYSTEM 120
300

FIG. 3

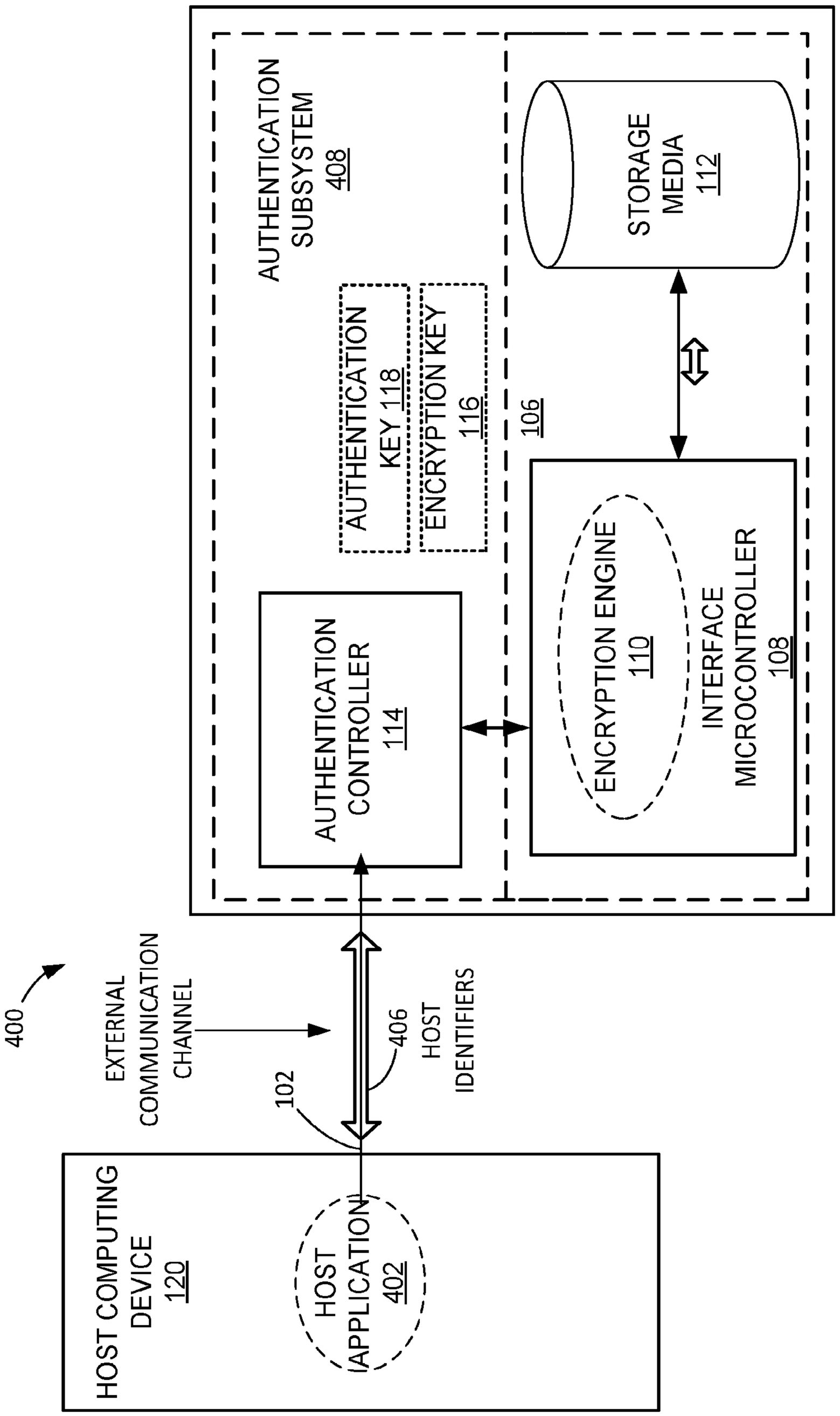

400
HOST COMPUTING DEVICE
120
HOST APPLICATION
402
102
EXTERNAL COMMUNICATION CHANNEL
406
HOST IDENTIFIERS
AUTHENTICATION SUBSYSTEM
408
AUTHENTICATION KEY
118
ENCRYPTION KEY
116
106
AUTHENTICATION CONTROLLER
114
ENCRYPTION ENGINE
110
INTERFACE MICROCONTROLLER
108
STORAGE MEDIA
112

FIG. 4

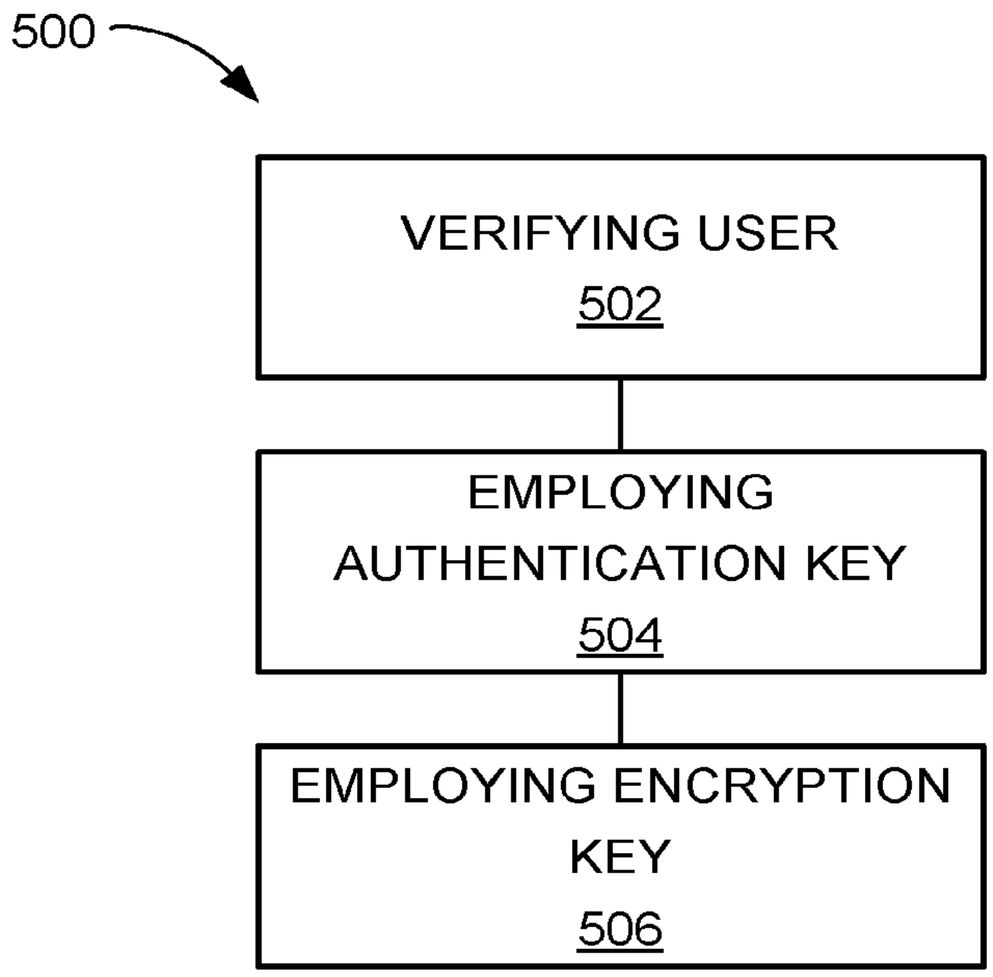

500
VERIFYING USER
502
EMPLOYING AUTHENTICATION KEY
504
EMPLOYING ENCRYPTION KEY
506

FIG. 5

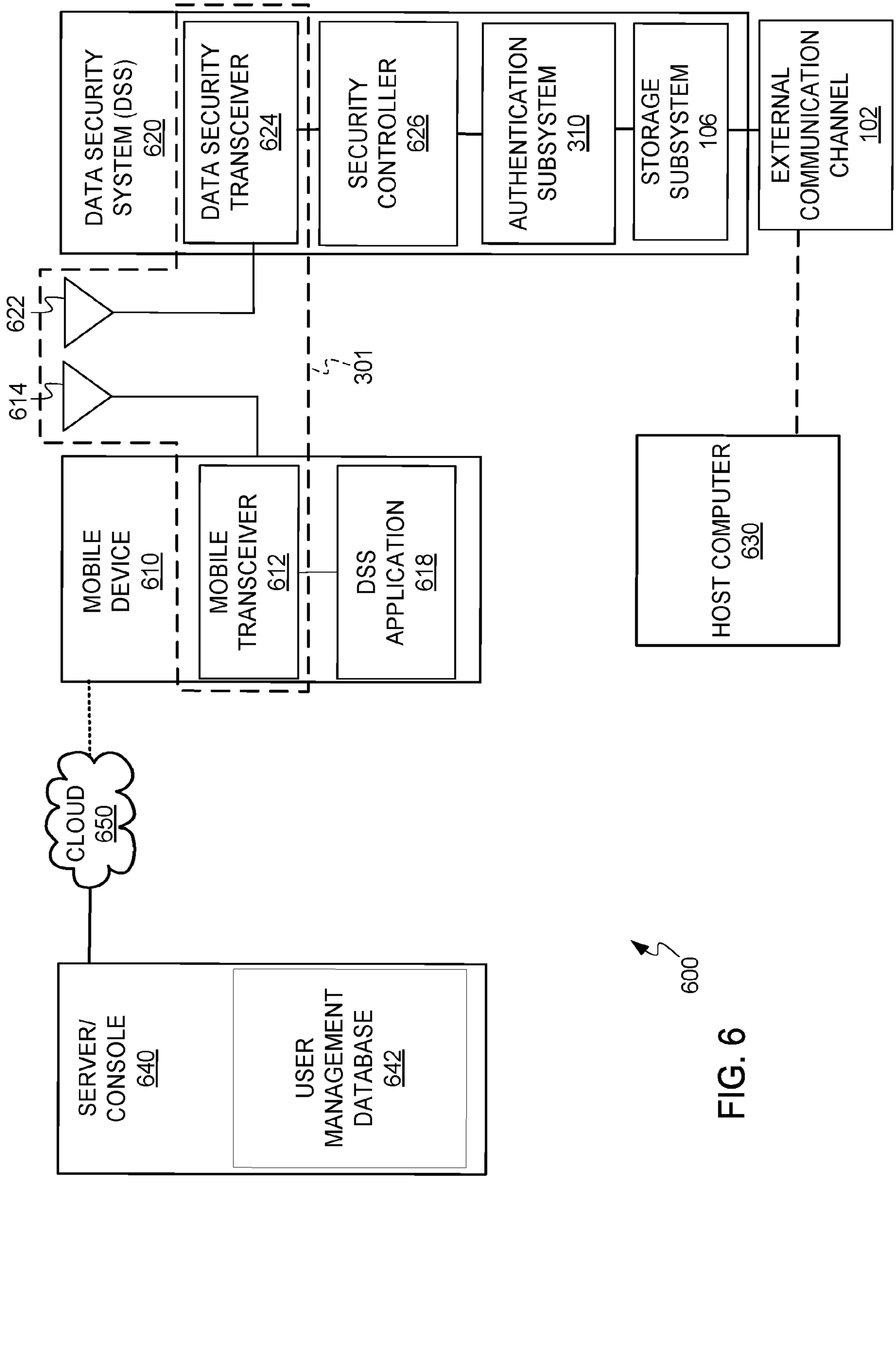

DATA SECURITY SYSTEM (DSS) 620
DATA SECURITY TRANSCEIVER 624
SECURITY CONTROLLER 626
AUTHENTICATION SUBSYSTEM 310
STORAGE SUBSYSTEM 106
EXTERNAL COMMUNICATION CHANNEL 102
622
614
301
MOBILE DEVICE 610
MOBILE TRANSCEIVER 612
DSS APPLICATION 618
HOST COMPUTER 630
CLOUD 650
SERVER/ CONSOLE 640
USER MANAGEMENT DATABASE 642
600

FIG. 6

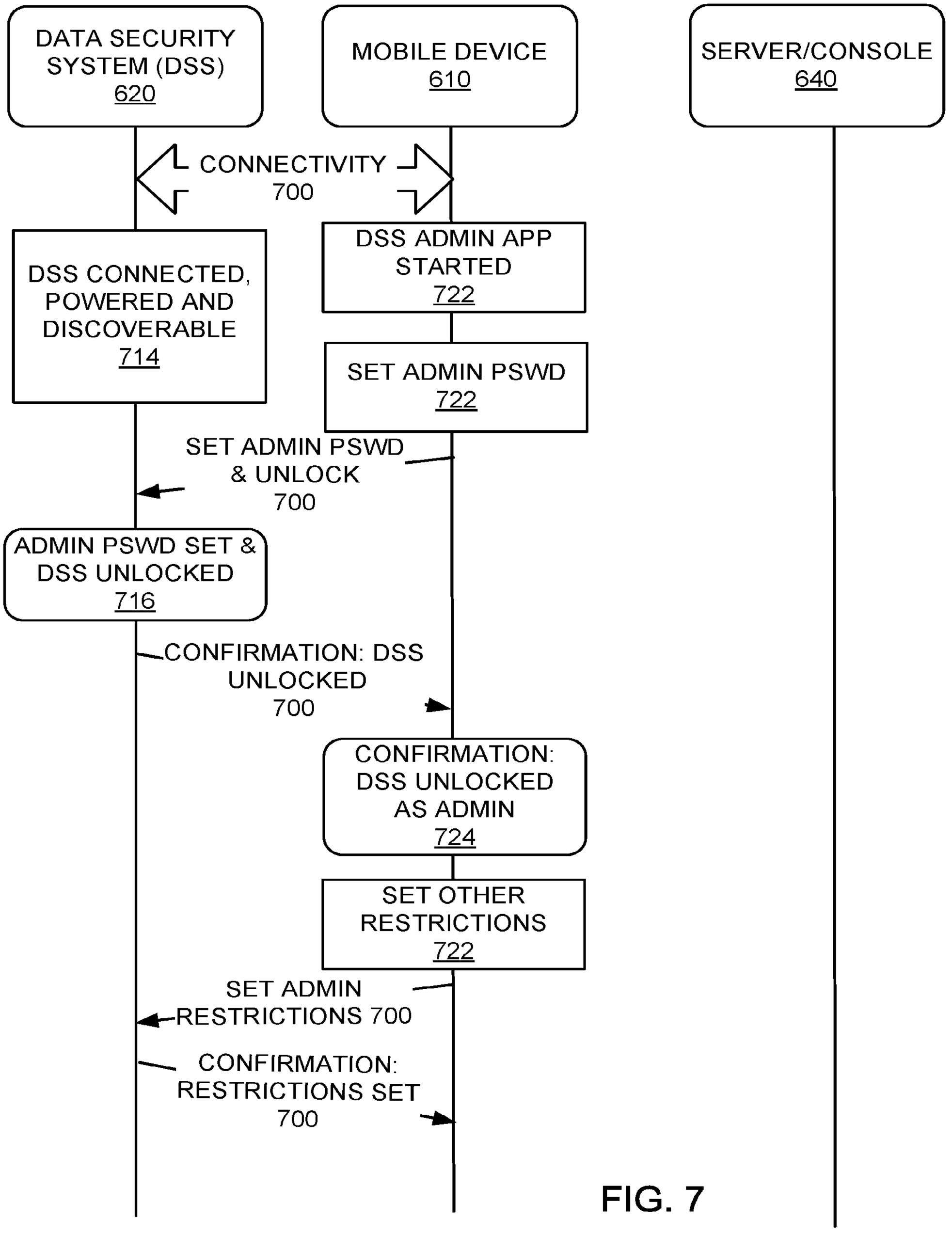

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 714
DSS ADMIN APP STARTED 722
SET ADMIN PSWD 722
SET ADMIN PSWD & UNLOCK 700
ADMIN PSWD SET & DSS UNLOCKED 716
CONFIRMATION: DSS UNLOCKED 700
CONFIRMATION: DSS UNLOCKED AS ADMIN 724
SET OTHER RESTRICTIONS 722
SET ADMIN RESTRICTIONS 700
CONFIRMATION: RESTRICTIONS SET 700

FIG. 7

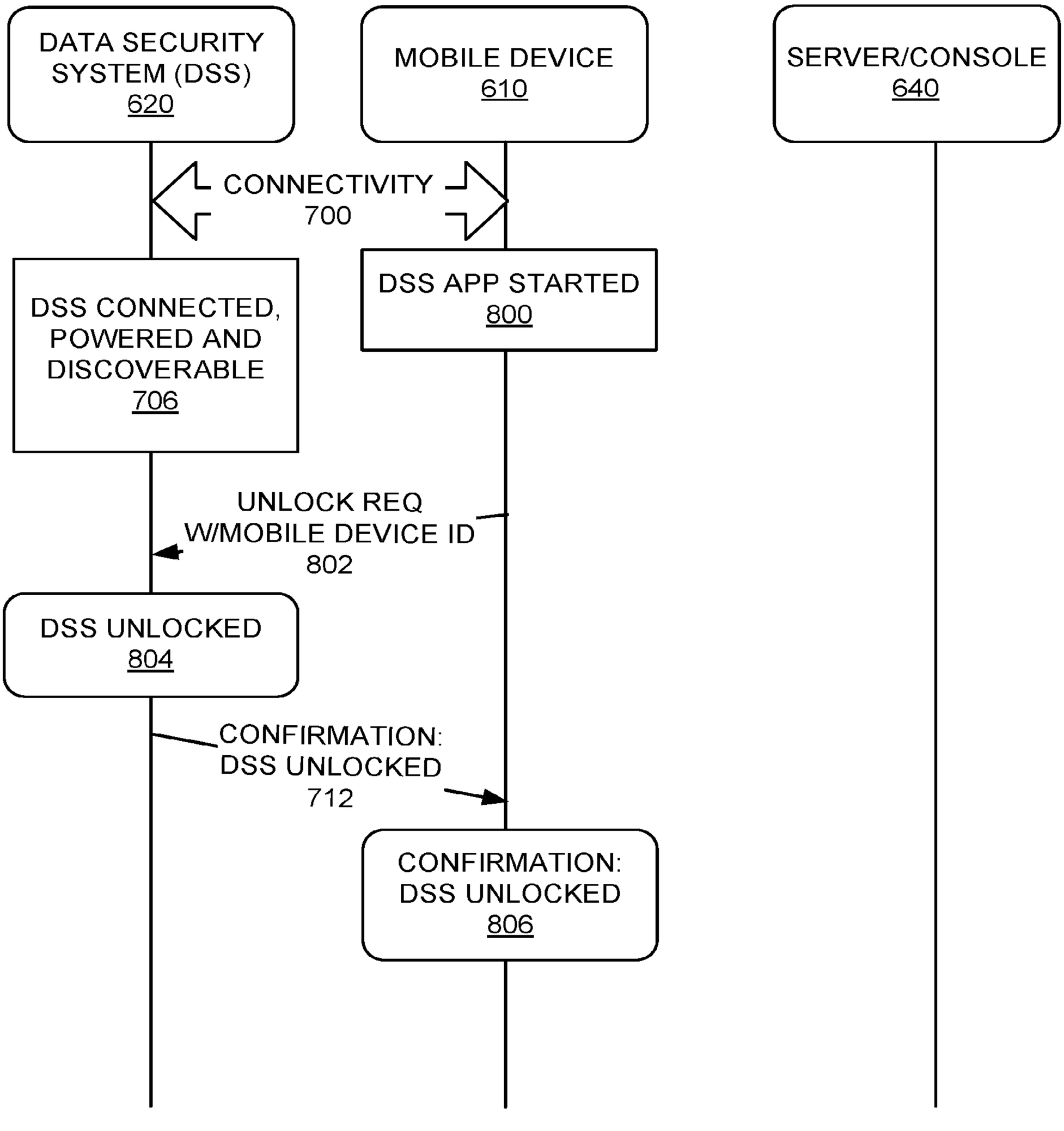

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 706
DSS APP STARTED 800
UNLOCK REQ W/MOBILE DEVICE ID 802
DSS UNLOCKED 804
CONFIRMATION: DSS UNLOCKED 712
CONFIRMATION: DSS UNLOCKED 806

FIG. 8

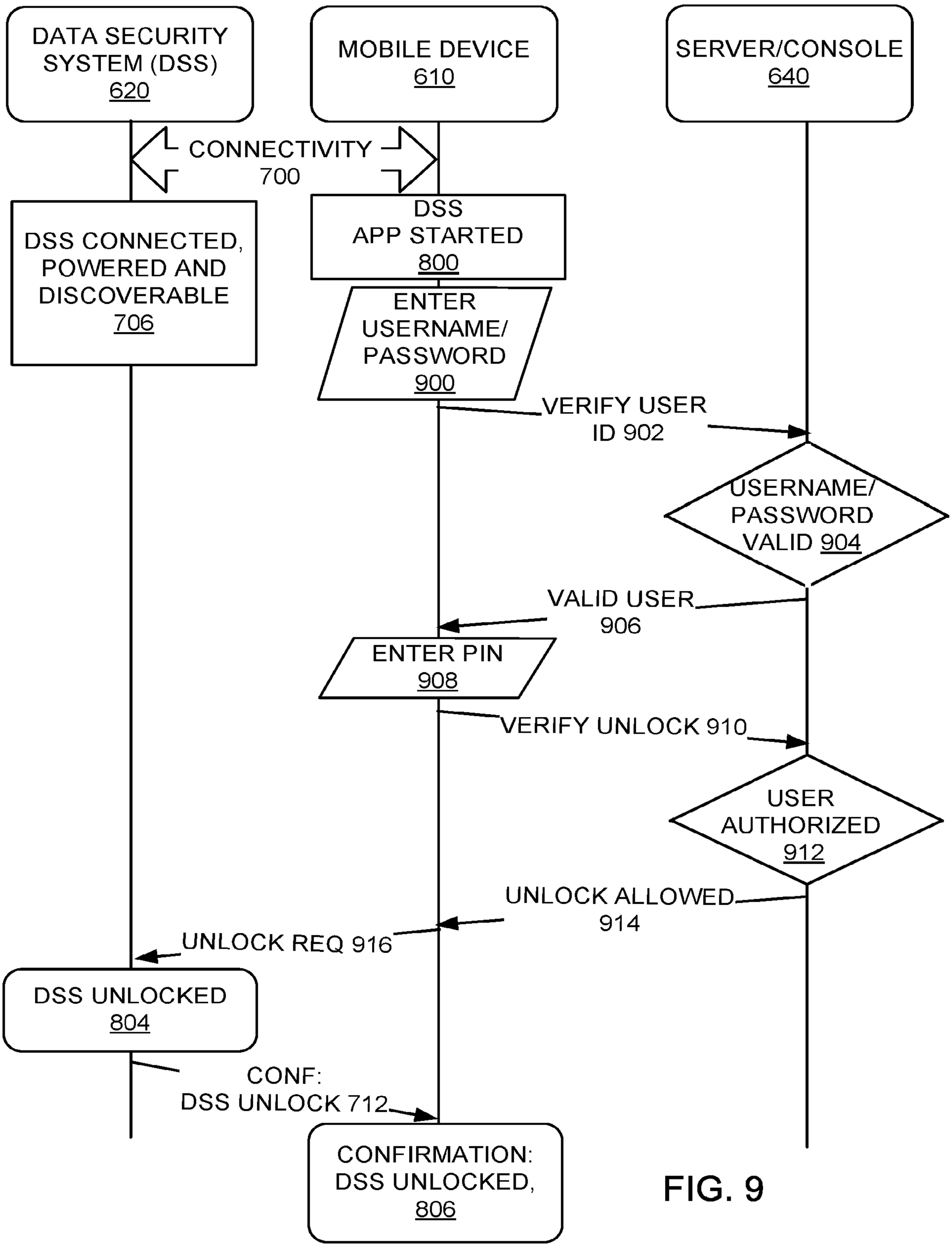

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 706
DSS APP STARTED 800
ENTER USERNAME/ PASSWORD 900
VERIFY USER ID 902
USERNAME/ PASSWORD VALID 904
VALID USER 906
ENTER PIN 908
VERIFY UNLOCK 910
USER AUTHORIZED 912
UNLOCK ALLOWED 914
UNLOCK REQ 916
DSS UNLOCKED 804
CONF: DSS UNLOCK 712
CONFIRMATION: DSS UNLOCKED, 806

FIG. 9

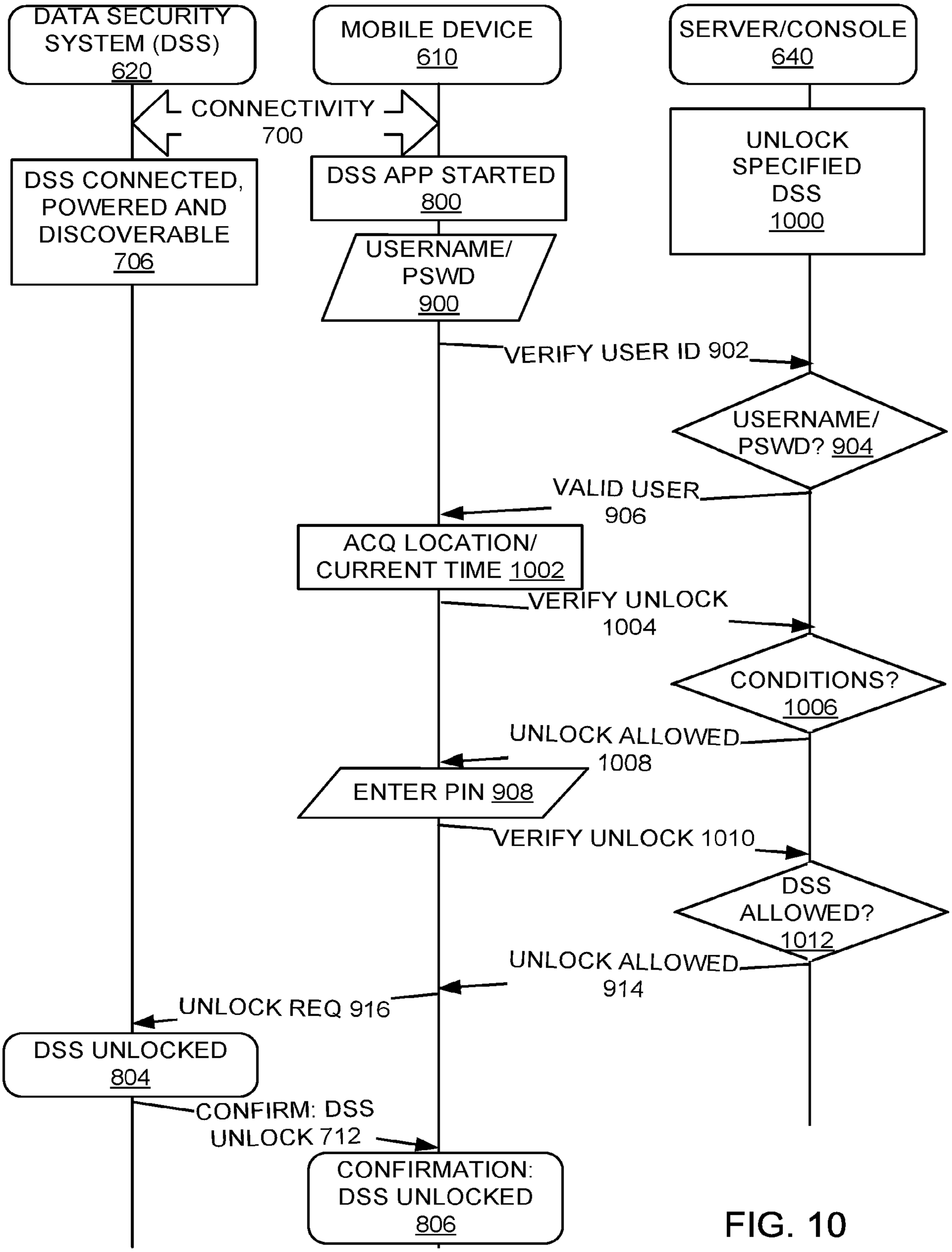

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 706
DSS APP STARTED 800
UNLOCK SPECIFIED DSS 1000
USERNAME/ PSWD 900
VERIFY USER ID 902
USERNAME/ PSWD? 904
VALID USER 906
ACQ LOCATION/ CURRENT TIME 1002
VERIFY UNLOCK 1004
CONDITIONS? 1006
UNLOCK ALLOWED 1008
ENTER PIN 908
VERIFY UNLOCK 1010
DSS ALLOWED? 1012
UNLOCK ALLOWED 914
UNLOCK REQ 916
DSS UNLOCKED 804
CONFIRM: DSS UNLOCK 712
CONFIRMATION: DSS UNLOCKED 806

FIG. 10

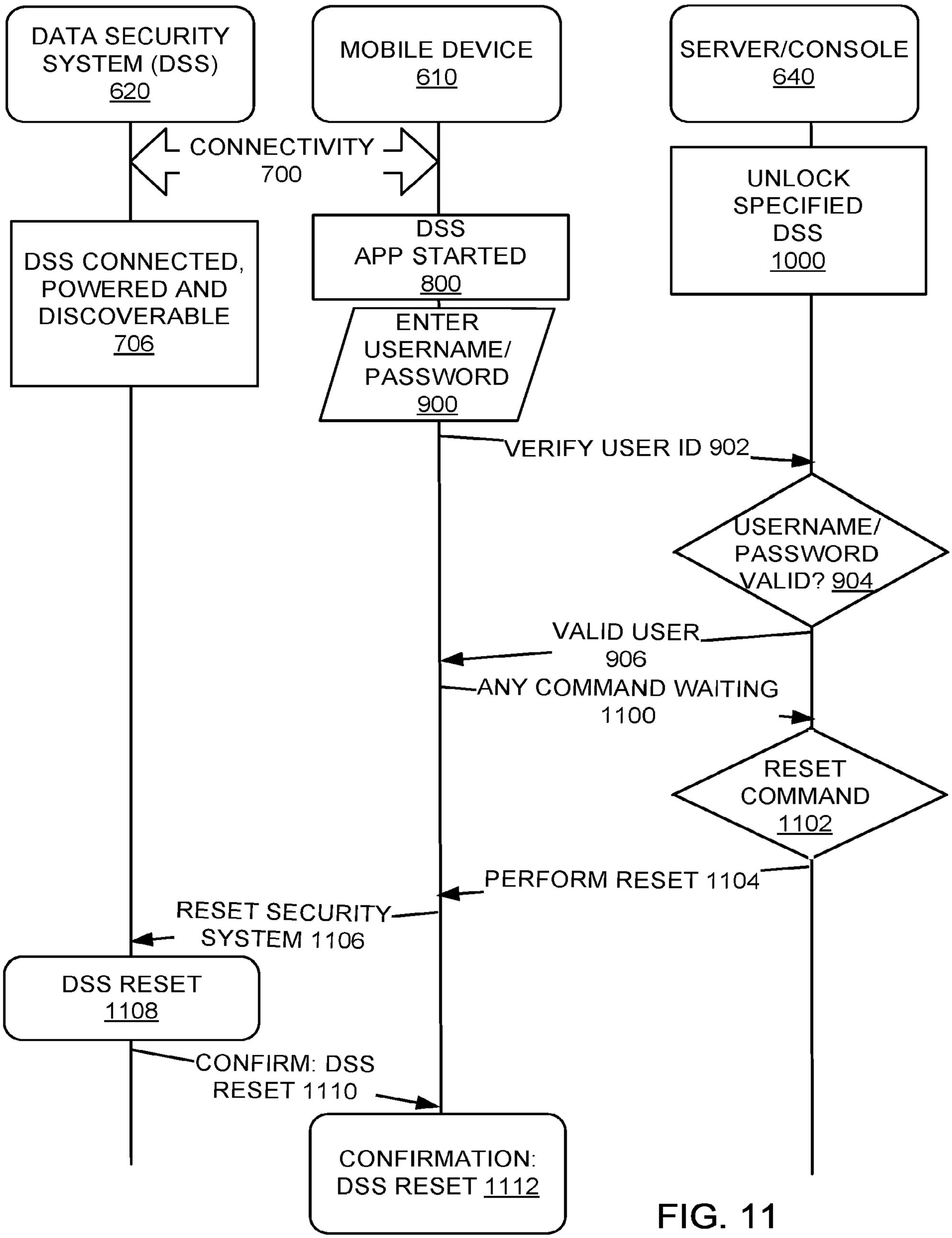

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 706
DSS APP STARTED 800
UNLOCK SPECIFIED DSS 1000
ENTER USERNAME/ PASSWORD 900
VERIFY USER ID 902
USERNAME/ PASSWORD VALID? 904
VALID USER 906
ANY COMMAND WAITING 1100
RESET COMMAND 1102
PERFORM RESET 1104
RESET SECURITY SYSTEM 1106
DSS RESET 1108
CONFIRM: DSS RESET 1110
CONFIRMATION: DSS RESET 1112

FIG. 11

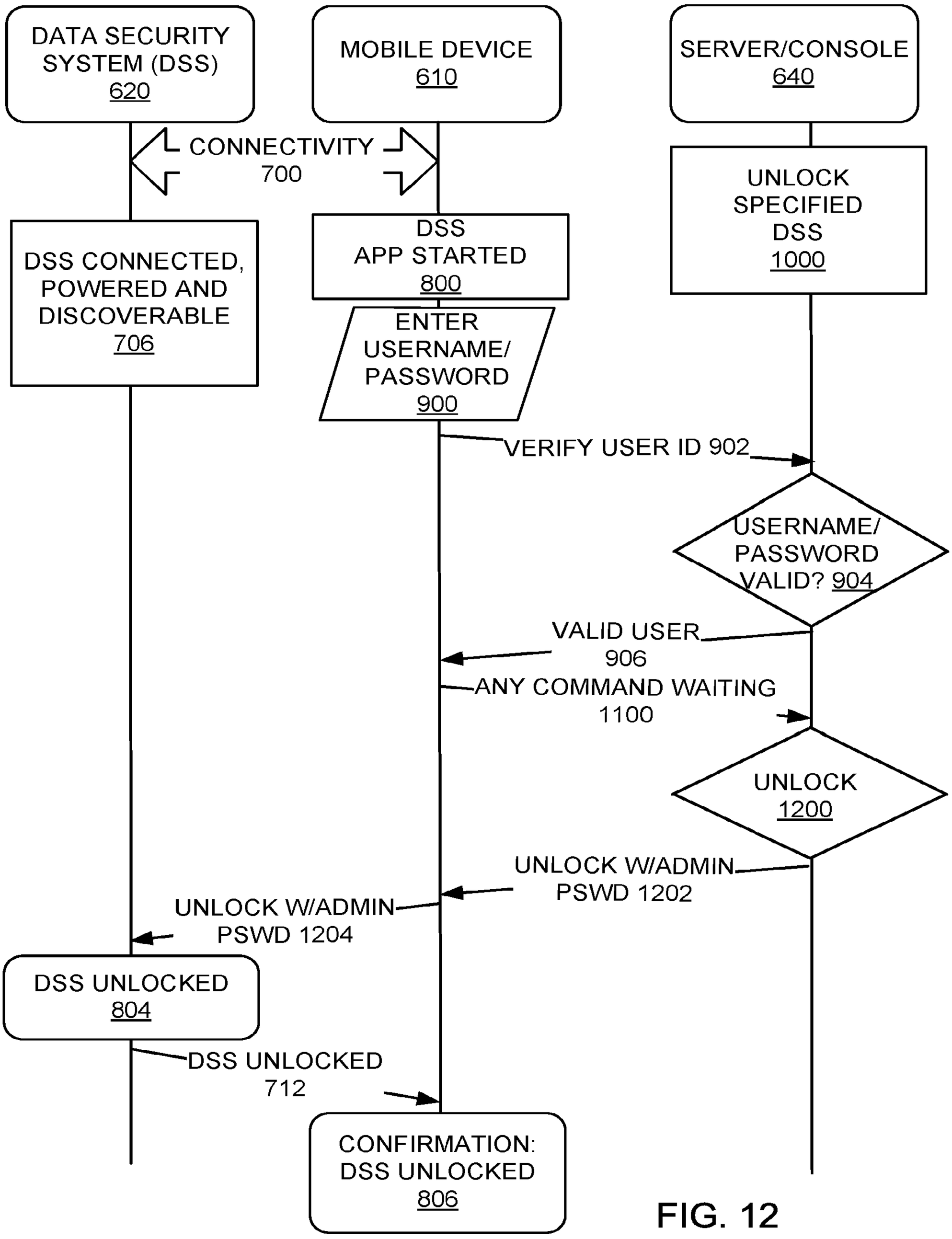

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 706
DSS APP STARTED 800
UNLOCK SPECIFIED DSS 1000
ENTER USERNAME/ PASSWORD 900
VERIFY USER ID 902
USERNAME/ PASSWORD VALID? 904
VALID USER 906
ANY COMMAND WAITING 1100
UNLOCK 1200
UNLOCK W/ADMIN PSWD 1202
UNLOCK W/ADMIN PSWD 1204
DSS UNLOCKED 804
DSS UNLOCKED 712
CONFIRMATION: DSS UNLOCKED 806

FIG. 12

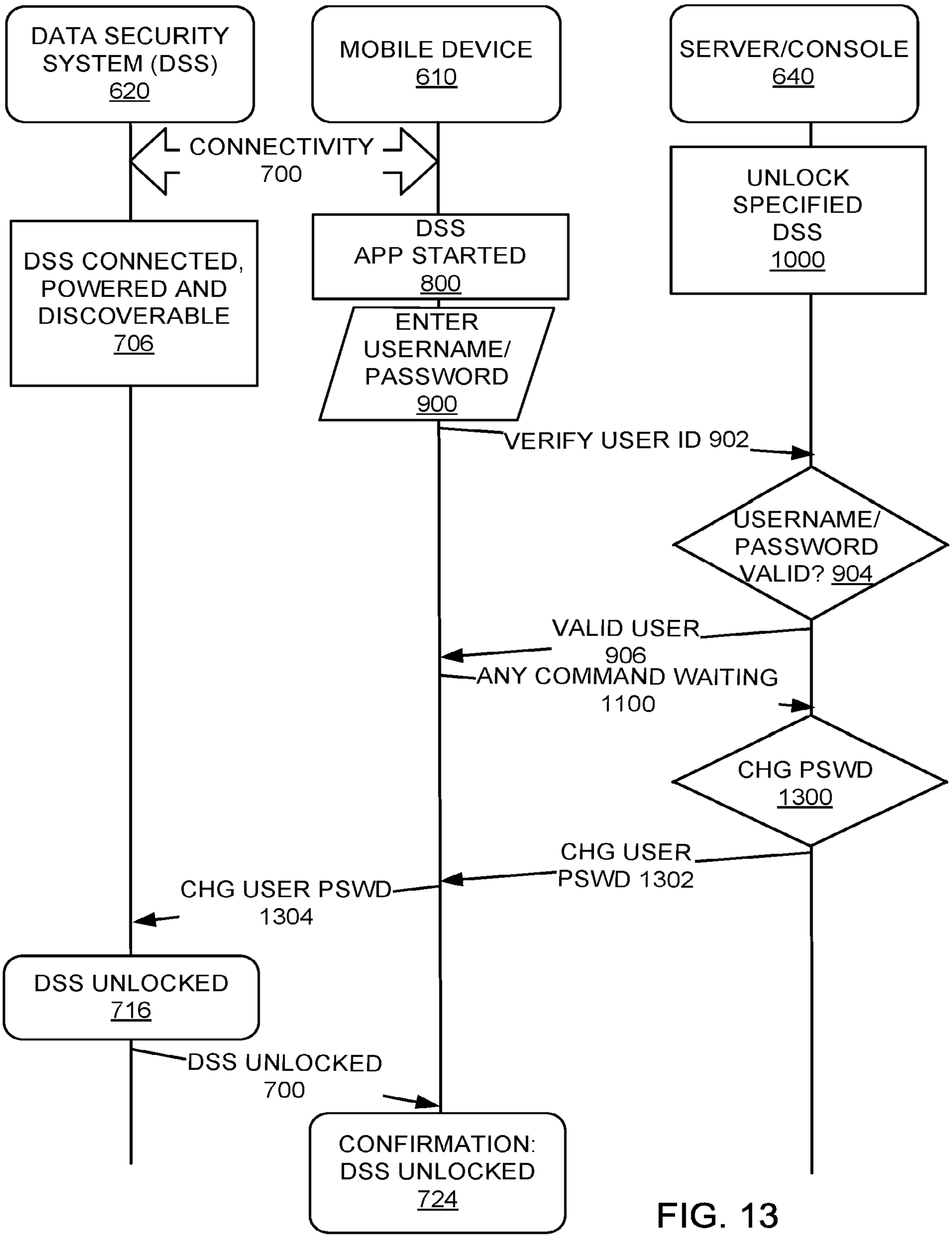

DATA SECURITY SYSTEM (DSS) 620
MOBILE DEVICE 610
SERVER/CONSOLE 640
CONNECTIVITY 700
DSS CONNECTED, POWERED AND DISCOVERABLE 706
DSS APP STARTED 800
ENTER USERNAME/ PASSWORD 900
UNLOCK SPECIFIED DSS 1000
VERIFY USER ID 902
USERNAME/ PASSWORD VALID? 904
VALID USER 906
ANY COMMAND WAITING 1100
CHG PSWD 1300
CHG USER PSWD 1302
CHG USER PSWD 1304
DSS UNLOCKED 716
DSS UNLOCKED 700
CONFIRMATION: DSS UNLOCKED 724

FIG. 13

Intellectual Property Office

The following terms are registered trade marks and should be read as such wherever they occur in this document:

iPod
Blu-ray
Firewire
Wi-Fi
Bluetooth
Touch ID
Apple Watch

DATA SECURITY SYSTEM WITH ENCRYPTION

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims priority of U.S. Patent Application number 14/987,749 filed January 4, 2016, which is a continuation-in-part of copending U.S. Patent Application number 12/680,742 filed March 29, 2010, which is the National Stage of International Application number PCT/US2008/077766 filed September 26, 2008, which claims the benefit of U.S. Provisional Patent Application serial number 60/975,814 filed September 27, 2007.

[0002] The present application contains subject matter related to a concurrently filed U.S. Patent Application by Lev M. Bolotin and Simon B. Johnson entitled "DATA SECURITY SYSTEM WITH ENCRYPTION". The related application is assigned to ClevX, LLC and is identified by docket number 502-018P-PCT-US.C1 (published as US2016/0119339 A1).

TECHNICAL FIELD

[0003] The present invention relates generally to electronic devices, and more particularly to memory devices.

BACKGROUND ART

[0004] Security is a critical issue with almost all aspects of computer use. Storage media, such as hard disk drives attached to computers, contain valuable information, which is vulnerable to data theft. A great deal of money and effort is being applied to guarding personal, corporate, and government security information.

[0005] As portable memory storage devices have become smaller, easier to lose, more ubiquitous, cheaper, and larger in memory capacity, they have come to pose extraordinary security problems. It is now possible to download massive amounts of information surreptitiously into portable memory storage devices, such as universal serial bus flash and micro drives, cellphones, camcorders, digital cameras, iPODs [RTM], MP3/4 players, smart phones, palm and laptop computers, gaming equipment, authenticators, tokens (containing memory), etc. – in general, a mass storage device (MSD).

[0006] More specifically, there are millions of MSDs being used for backup, transfer, intermediate storage, and primary storage into which information can be easily downloaded from a computer and carried away. The primary purpose of any MSD is to store and retrieve "portable content," which is data and information tied to a particular owner not a particular computer.

[0007] The most common means of providing storage security is to authenticate the user with a computer-entered password. A password is validated against a MSD stored value. If a match occurs, the drive will open. Or, the password itself is used as the encryption key to encrypt / decrypt data stored to the MSD.

[0008] For drives that support on-the-fly encryption, the encryption key is often stored on the media in an encrypted form. Since the encryption key is stored on the media, it becomes readily available to those willing to circumvent the standard interface and read the media directly. Thus, a password is used as the key to encrypt the encryption key.

[0009] For self-authenticating drives, their authentication sub-system is responsible for maintaining security. There is no dependency on a host computer to which it is connected. Thus, a password cannot (or need not) be sent from the host in order to unlock the MSD. In fact, the encryption key no longer needs to be stored on the media. The authentication subsystem becomes the means for managing encryption keys.

[0010] Thus, a need still remains for improved security. In view of the ever-increasing commercial competitive pressures, along with growing consumer expectations and the diminishing opportunities for meaningful product differentiation in the marketplace, it is critical that answers be found for these problems. Additionally, the need to reduce costs, improve efficiencies and performance, and meet competitive pressures, adds an even greater urgency to the critical necessity for finding answers to these problems.

[0011] Solutions to these problems have been long sought but prior developments have not taught or suggested any solutions and, thus, solutions to these problems have long eluded those skilled in the art.

DISCLOSURE OF THE INVENTION

[0012] The present invention provides a method of operation of a data security system including: providing a mobile device with a data security system application for connectivity with the data security system; starting the data security system application; and maintaining connectivity of the data security system with the mobile device.

[0013] The present invention provides a data security system including: a data security transceiver or receiver; an authentication subsystem operatively connected to the data security transceiver or receiver; and a storage subsystem connected to the authentication subsystem.

[0014] Certain embodiments of the invention have other aspects in addition to or in place of those mentioned above. The aspects will become apparent to those skilled in the art from a reading of the following detailed description when taken with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. 1 is a schematic of a data security system in accordance with an embodiment of the present invention;

[0016] FIG. 2 is an illustration of an authentication key delivery method used with the data security system;

[0017] FIG. 3 is an illustration of different systems for the user to interact with the data security system;

[0018] FIG. 4 is an illustration of how the user can employ the host computer system to interact with a data security system; and

[0019] FIG. 5 is a data security method employing user verification for the data security system.

[0020] FIG. 6 is an exemplary data security communication system.

[0021] FIG. 7 is an administrator sequencing diagram showing the sequence of operations between a mobile device and the data security system.

[0022] FIG. 8 is a unlocking sequence diagram where the mobile device is an authentication factor.

[0023] FIG. 9 is an unlock sequencing diagram showing unlocking using a PIN entry from the mobile device.

[0024] FIG. 10 is an unlock sequencing diagram showing unlock using a PIN entry and User ID/location/time verification via the server/console.

[0025] FIG. 11 is a reset sequencing diagram showing resetting the data security system using a server/console.

[0026] FIG. 12 is an unlock sequencing diagram showing unlocking the data security system using the server/console.

[0027] FIG. 13 is a change user's password sequencing diagram using the server/console.

BEST MODE FOR CARRYING OUT THE INVENTION

[0028] The following embodiments are described in sufficient detail to enable those skilled in the art to make and use the invention. It is to be understood that other embodiments would be evident based on the present disclosure, and that system, process, or mechanical changes may be made without departing from the scope of the present invention.

[0029] In the following description, numerous specific details are given to provide a thorough understanding of the invention. However, it will be apparent that the invention may be practiced without these specific details. In order to avoid obscuring the present invention, some well-known circuits, system configurations, and process steps are not disclosed in detail.

[0030] Likewise, the drawings showing embodiments of the system are semi-diagrammatic and not to scale and, particularly, some of the dimensions are for the clarity of presentation and are shown exaggerated in the drawing FIGs. Where multiple embodiments are disclosed and described having some features in common, for clarity and ease of illustration, description, and comprehension thereof, similar and like features one to another will ordinarily be described with similar or the same reference numerals. Similarly, although the views in the drawings for ease of description generally show similar orientations, this depiction in the FIGs. is arbitrary for the most part. Generally, the invention can be operated in any orientation.

[0031] The term "system" as used herein refers to and is defined as the method and as the apparatus of the present invention in accordance with the context in which the term is used. The term "method" as used herein refers to and is defined as the operational steps of an apparatus.

[0032] For reasons of convenience and not limitation, the term "data" is defined as information that is capable of being produced by or stored in a computer. The term "data security system" is defined as meaning any portable memory device incorporating a storage medium. The term "storage media" as used herein refers to and is defined as any solid state, NAND Flash, and/or magnetic data recording system. The term "locked" refers to the data security system when the storage media is not accessible and the term "unlocked" refers to the data security system when the storage media is accessible.

[0033] There are generally two methods to make a storage device tamper resistant:

1. Apply epoxy to components – an epoxy resin applied to the printed circuit board can make it difficult to disassemble the storage device without destroying storage media.

2. Encrypt memory data – data gets encrypted as it is written to the storage media and an encryption key is required to decipher the data.

[0034] Referring now to FIG. 1, therein is shown a schematic of a data security system 100 in accordance with an embodiment of the present invention. The data security system 100 consists of an external communication channel 102, an authentication subsystem 104, and a storage subsystem 106.

[0035] The storage subsystem 106 is electronic circuitry that includes an interface controller 108, an encryption engine 110, and a storage media 112. The storage media 112 can be an internal or external hard disk drive, USB flash drive, solid state drive, hybrid drive, memory card, tape cartridge, and optical media including optical disk (e.g., Blu-ray [RTM] disk, digital versatile disk or DVD, and compact disk or CD). The storage media 112 can include a data protection appliance, archival storage system, and cloud-based data storage system. The cloud storage system may be accessed utilizing a plug-in (or "plugin") application or extension software installed in a browser application, either on the host computer or on another system coupled to the host computer via a wired or wireless network, such as RF or optical, or over the world wide web.

20 29 05

[0036] The interface controller 108 includes electronic components such as a micro-controller with the encryption engine 110 of software or hardware, although the encryption engine 110 can be in a separate controller in the storage subsystem 106.

[0037] The authentication subsystem 104 is electronic circuitry that includes an authentication controller 114, such as a micro-controller, which may have its own non-volatile memory, such as an electrically erasable programmable read-only memory (EEPROM).

[0038] The external communication channel 102 provides a means of exchanging data with a host computer system 120. Universal Serial Bus (USB) is one of the most popular means to connect the data security system 100 to the host computer system 120. Other examples of the external communication channel 102 include Firewire [RTM], wireless USB, Serial ATA (SATA), High Definition Multimedia Interface (HDMI), Recommended Standard 232 (RS-232), and radio frequency wireless networks.

[0039] The interface controller 108 is capable of translating USB packet data to data that can be written to the storage media 112 in a USB Flash Drive.

[0040] The encryption engine 110 is implemented as part of the interface controller 108 and takes clear text and/or data (information) from the host computer system 120 and converts it to an encrypted form that is written to the MSD or the storage media 112. The encryption engine

110 also converts encrypted information from the storage media 112 and decrypts it to clear information for the host computer system 120. The encryption engine 110 can also be a two controller subsystem with an encryption controller that has the encryption capability to encrypt/decrypt data on the fly along with managing the communication protocol, memory, and other operating conditions and a communication/security controller for handling the communication, encryption key management, and communications with the encryption controller.

[0041] An encryption key 116 is required by the encryption engine 110 to encrypt / decrypt the information. The encryption key 116 is used in an algorithm (e.g., a 256 bit Advanced Encryption Standard (AES) encryption) that respectively encrypts / decrypts the data by an encryption algorithm to render data unreadable or readable. The encryption key 116 can be stored either internally or externally to the authentication controller 114.

[0042] The encryption key 116 is transmitted to the encryption engine 110 by the authentication subsystem 104 once a user 122, having an identification number or key, has been verified against an authentication key 118.

[0043] It has been discovered that, by the employment of the authentication key 118 and the encryption key 116, portable memory storage devices of the various embodiments of the present invention can be provide an extremely high level of security previously not available in such devices.

[0044] When the data security system 100 is locked, the authentication key 118 remains inside the authentication subsystem 104 and cannot be read from outside. One method of hiding the authentication key 118 is to store it in the authentication controller 114 in the authentication subsystem 104. Setting the security fuse of the authentication controller 114 makes it impossible to access the authentication key 118 unless the authentication controller 114 allows retrieval once the user 122 has been verified. Many micro-controllers come equipped with a security fuse that prevents accessing any internal memory when blown. This is a well-known and widely used security feature. Such a micro-controller could be used for the authentication controller 114. The authentication controller 114 can be a micro-controller or microprocessor.

[0045] The authentication key 118 can be used as in several capacities:

1. As the encryption key 116 to encrypt/decrypt the information directly.
2. As a key to recover the encryption key 116 stored in the data security system 100 that can be accessed by the interface controller 108.

3. Used for direct comparison by the interface controller 108 to activate the external communication channel 102.

[0046] Referring now to FIG. 2, therein is shown an illustration of an authentication key delivery method used with the data security system 100. In this illustration, the authentication key 118 and the encryption key 116 are one and the same. The encryption engine 110 employs the authentication key 118 as the encryption key 116.

[0047] The user 122 must interact with the authentication subsystem 104 by providing user identification 202, a number or key, to the authentication subsystem 104. The authentication subsystem 104 validates the user 122 against the authentication key 118. The authentication subsystem 104 then transmits the authentication key 118 as the encryption key 116 to the interface controller 108.

[0048] The encryption engine 110 in the interface controller 108 employs the authentication key 118 to convert clear information to encrypted information and encrypted information to clear information along a channel 206. Any attempt to read encrypted information from the storage media 112 without the encryption key 116 will generally result in information that is unusable by any computer.

[0049] Referring now to FIG. 3, therein is shown an illustration of different systems for the user 122 to interact with a data security system 300. The interaction can be by a communication combination 301, which can be by a physical contact, wired connection, or wireless connection from a cell phone, smartphone, smart watch, wearable appliance, or other wireless device.

[0050] In one authentication system, a mobile transceiver 302 is employed to transmit user identification 304 to a data security transceiver 306 in an authentication subsystem 310. For exemplary purposes, transceivers are employed for bi-directional communication flexibility but a transmitter-receiver combination for uni-directional communication could also be used. The authentication subsystem 310 includes the authentication controller 114, which is connected to the interface controller 108 in the storage subsystem 106. The user identification 304 is supplied to the data security transceiver 306 within the authentication subsystem 310 by the mobile transceiver 302 from outside the storage subsystem 106 of the data security system 300. The wireless communication may include Wireless Fidelity (Wi-Fi[RTM]), Bluetooth [RTM] (BT), Bluetooth Smart, Near Field Communication (NFC), Global Positioning System (GPS), optical, cellular communication (for example, Long-Term Evolution (LTE), Long-Term Evolution Advanced (LTE-A)), Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Universal Mobile Telecommunications System

20 29 05

(UMTS), Wireless Broadband (WiBro), or Global System for Mobile Communications (GSM), and the like).

[0051] The authentication subsystem 310 validates the user 122 against the authentication key 118 by a code sent from the mobile transceiver 302 being validated against the authentication key 118. The authentication subsystem 310 then transmits the encryption key 116 to the interface controller 108 across the communication combination 301.

[0052] The encryption engine 110 then employs the encryption key 116 to convert clear information to encrypted information and encrypted information to clear information along the channel 206. Any attempt to read encrypted information from the storage media 112 without the encryption key 116 will result in information that is unusable by the host computer system 120.

[0053] In an optional second authentication mechanism, the authentication subsystem 310 validates the user 122 against the authentication key 118 by having the user 122 employ a biometric sensor 320 to supply a biometric input 322 to verify his/her identity as an authorized user. Types of biometric identification include a fingerprint, an iris scan, a voice imprint, etc.

[0054] In an optional third authentication mechanism, The authentication subsystem 310 validates the user 122 against the authentication key 118 by having the user 122 employ an electro-mechanical input mechanism 330 to supply a unique code 332 to verify his/her identity as an authorized user. The unique code 332 can include a numerical, alphanumeric, or alphabetic code, such as a PIN. The electro-mechanical input mechanism 330 is within the authentication subsystem 310. The electro-mechanical input mechanism 330 receives the unique code 332 from the user 122 from outside of the data security system 300. The unique code 332 is supplied to the electro-mechanical input mechanism 330 within the authentication subsystem 310 from outside the storage subsystem 106 of the data security system 300.

[0055] No matter which method is used to validate the user 122, the authentication key 118 and the encryption key 116 remain hidden until the user 122 is authenticated.

[0056] Referring now to FIG. 4, therein shows an illustration of how the user 122 can employ the host computer system 120 to interact with a data security system 400.

[0057] The host computer system 120 is provided with a host application 402. The host application 402 is software or firmware, which communicates over the external communication channel 102 of the data security system 400.

[0058] The host application 402 delivers host identifiers 406, such as internal component serial numbers (e.g. hard drive), media access control (MAC) address of a network card, login

name of the user, network Internet Protocol (IP) address, an ID created by the data security system and saved to the host, an ID created by the data security system and saved to the network, etc., associated with its environment. The host identifiers 406 are employed by an authentication subsystem 408 in the data security system 400.

[0059] When the authentication subsystem 408 validates the user 122 against the authentication key 118 by verifying the host identifiers 406, the data security system 400 will unlock.

[0060] For example, the user 122 connects the data security system 400 that is locked to the host computer system 120. The host application 402 sends the MAC address of its network card to the data security system 400. The data security system 400 recognizes this MAC address as legitimate and unlocks without the user 122 of FIG. 1 having to enter user identification. This is implementation does not require any interaction with the user 122. In this case, it is the host computer system 120 and its associated environment that are being validated.

[0061] The data security system 400 includes: providing the authentication key 118 stored in the authentication subsystem 104; providing verification of the host computer system 120 by the authentication subsystem 104; presenting the encryption key 116 to the storage subsystem 106 by the authentication subsystem 104; and providing access to the storage media 112 by the storage subsystem 106 by way of decrypting the storage media content.

[0062] The data security system further includes the authentication subsystem 104 for interpretation of biometric input and verification of the user 122.

[0063] The data security system further includes using the authentication key 118 as the encryption key 116 directly.

[0064] The data security system further includes using the authentication key 118 to decrypt and retrieve the encryption key 116 used to decipher internal content.

[0065] The data security system further includes the authentication subsystem 104 for interpretation of signal inputs and verification of sending unit.

[0066] The data security system further includes the authentication subsystem 104 for interpretation of manually entered input and verification of the user 122.

[0067] The data security system further includes the authentication subsystem 104 for interpretation of input sent by a host resident software application for verification of the host computer system 120.

[0068] The data security system as further includes the encryption engine 110 outside the interface controller 108 but connected to the external communication channel 102 for the purpose of converting clear data to encrypted data for unlocking the data security system 100.

[0069] Referring now to FIG. 5, therein is shown a data security method 500 employing user verification for the data security system 100. The data security method 500 includes; verifying the user against an authentication key in a block 502; employing the authentication key for retrieving an encryption key in a block 504; and employing the encryption key for allowing unencrypted communication through a storage subsystem between a host computer system and a storage media in a block 506.

[0070] Referring now to FIG. 6, therein is shown an exemplary data security communication system 600. The exemplary data security communication system 600 includes a mobile device 610, a data security system 620, a host computer 630, and a server/console 640. The mobile device 610 and the server/console 640 are connected by wired or wireless connections through a cloud 650, which can be an Internet cloud. The mobile device 610 and the data security system 620 are connected by the communication combination 301.

[0071] The communication combination 301 in the exemplary data security communication system 600 includes a mobile transceiver 612 in the mobile device 610 with an antenna 614 wirelessly communicating with an antenna 622 of a data security transceiver 624 in the data security system 620.

[0072] The mobile device 610 in one embodiment can be a smartphone. In the mobile device 610, the mobile transceiver 612 can be connected to conventional mobile device components and to a data security system application 618, which provides information to be used with the data security system 620.

[0073] The data security transceiver 624 is connected to a security controller 626, which can contain identification, passwords, profiles, or information including that of different mobile devices that can access the data security system 620. The security controller 626 is connected to subsystems similar to the authentication subsystem 310, the storage subsystem 106 (which in some embodiments can have encryption to encrypt data), and the external communication channel 102.

[0074] The external communication channel 102 is connectible to the host computer 630 to allow, under specified circumstances, access to data in the storage subsystem 106.

[0075] One implementation of the data security system 620 can eliminate the biometric sensor 320 and the electro-mechanical input mechanism 330 of FIG. 3 with only a wireless link

to the mobile device 610, such as a smartphone. It has been found that this implementation makes the data security system 620 more secure and useful.

[0076] The data security system application 618 allows the mobile device 610 to discover all data security systems in the vicinity of the mobile device 610 and show their status (locked/unlocked/blank, paired/unpaired etc.).

[0077] The data security system application 618 allows the mobile device 610 to connect/pair, lock, unlock, change the name and password, and reset all data on the data security system 620.

[0078] The data security system application 618 allows the mobile device 610 to set an inactivity auto-lock so the data security system 620 will automatically lock after a predetermined period of inactivity or to set a proximity auto-lock so the data security system 620 will be locked when the mobile device 610 is not within a predetermined proximity for a predetermined time period (to improve reliability and avoid signal de-bouncing).

[0079] The data security system application 618 allows the mobile device 610 to remember a password, use TouchID [RTM], and Apple Watch [RTM] (both TouchID and Apple Watch mentioned here as examples only, there are many other mobile devices with biometric sensors and wearables that can be used in a similar mode) so data security system 620 could be unlocked without entering re-entering a password on the mobile device

[0080] The data security system application 618 allows the mobile device 610 to be set to operate only with a specific mobile device, such as the mobile device 610, so the data security system 620 cannot be unlocked with other mobile devices (1Phone).

[0081] The data security system application 618 allows the mobile device 610 to set the data security system 620 to Read-Only

[0082] The data security system application 618 allows the mobile device 610 to operate in User Mode or Administrator Mode (administrator's mode overrides user's settings) and use the server/console 640. The server/console 640 is a combination of a computer with a console for entering information into the computer.

[0083] The server/console 640 contains a user management database 642, which contains additional information that can be transmitted over the cloud 650 to the mobile device 610 to provide additional functionality to the mobile device 610.

[0084] The user management database 642 allows the server/console 640 to create and identify users using UserID (username and password) and block/allow unlocking the data security system 620 and provide remote help.

20 29 05

[0085] The user management database 642 allows the server/console 640 to remotely reset or unlock the data security system 620.

[0086] The user management database 642 allows the server/console 640 to remotely change the data security system user's PIN.

[0087] The user management database 642 allows the server/console 640 to restrict/allow unlocking data security system 620 from specific locations (by using geo-fencing)

[0088] The user management database 642 allows the server/console 640 to restrict/allow unlocking data security system 620 in specified time periods and different time zones

[0089] The user management database 642 allows the server/console 640 to restrict unlocking data security system 620 outside of specified team/organization/network etc.

[0090] Referring now to FIG. 7, therein is shown an administrator sequencing diagram showing the sequence of operations between the mobile device 610 and the data security system 620.

[0091] Connectivity 700, between the data security system 620 and the mobile device 610, is first established with mutual discovery of the other device or system, pairing the device and system, and connection of the device and system. The connectivity 700 is secured using a shared secret, which is then used to secure (encrypt) communications between the data security system 620 and the mobile device 610 for all future communication sessions. A standard encryption algorithm is selected to be both efficient to run on the data security system 620 and to be approved by world-wide security standards.

[0092] The connectivity 700 is maintained by the data security system application 618 or the security controller 628 or both operating together as long as the data security system 620 and the mobile device 610 are within a predetermined distance of each other. Further, if the predetermined distance is exceeded, the connectivity 700 is maintained for a predetermined period of time after which the data security system 620 is locked.

[0093] After connection of the mobile device 610 and the data security system 620, a data security system administrator application start operation 702 occurs in the mobile device 610. Then an administrator sets a password in an administrator password operation 704. Also after connection of the mobile device 610 and the data security system 620, the data security system 620 is connected to the host computer 630 of FIG. 6 to be powered up and discoverable by the host computer 630 in a data security system connected, powered and discoverable operation 706.

[0094] After the administrator password operation 704, the mobile device 610 sends a set administrator password and unlock signal 708 to the data security system 620. The set administrator password and unlock signal 708 causes an administrator password set and data security system unlocked operation 716 to occur in the data security system 620.

[0095] When the administrator password set and data security system unlocked operation 716 is completed, a confirmation: data security system unlocked signal 712 is sent to the mobile device 610 where a confirmation: data security system unlocked as administrator operation 714 operates. The confirmation: data security system unlocked as administrator operation 714 permits a set other restrictions operation 716 to be performed using the mobile device 610. The set other restrictions operation 716 causes a set administrator restrictions signal 718 to be sent to the data security system 620 where the administrator restrictions are set and a confirmation: restrictions set signal 720 is returned to the mobile device 610. Thereafter, the mobile device 610 and the data security system 620 are in full operative communication.

[0096] Because it is possible to communicate with the data security system 620 without having physical contact with the data security system 620, it is required that significant interactions with the data security system 620 be accompanied by a data security system unique identifier that is either printed on the data security system 620 itself, or that comes with the data security system 620 packaging and is readily available to the data security system 620 owner.

[0097] On making requests that could affect user data, such as unlocking or resetting the data security system 620, this unique identifier (unique ID) is required. Attempts to perform these operations without the correct identifier are ignored and made harmless. The unique identifier is used to identify the data security system 620 to the mobile device 610 in a way that requires the user to have physical control over the data security system 620 and to verify the connectivity 700 is established between the authorized, previously paired device and system, such as the mobile device 610 and the data security system 620. Once the devices are paired, the shared secret is used to make the communication confidential.

[0098] Pairing connotes that a mobile device and a data security system have a unique and defined relationship established at some time in the past and enduring.

[0099] The unique identifier makes for giving the user some control over the data security system when the user has physical control of the data security system.

[00100] To increase the security of the communication with the data security system 620 where the mobile device 610 is a smartphone, a user may choose to enable a feature, such as a

feature called 1Phone here. This feature restricts significant user interactions with the data security system 620 to one and only one mobile device 610. This is done by replacing the data security system unique identifier described above with a random identifier shared securely between the data security system 620 and the mobile device 610. So, instead of presenting the data security system unique identifier when, for example, the user unlocks the data security system 620, the 1Phone identifier must be given instead. In effect, this makes the user's mobile device 610 a second authentication factor for using the data security system 620 in addition to a PIN or password. As an example, the paired user phone selected as “1Phone” can be used without a PIN, and as the user-authentication single factor and/or in a combination with any other user-authentication factors. If such feature (1Phone) is selected, the data security system 620 cannot be open with any other phones, except if an administrator’s unlock was enabled before.

[00101] It will be understood that other embodiments can be made to require an administrat’r's password on the data security system 620 in order to use the 1Phone feature. Another embodiment may require that the server/console 640 is capable of recovering the data security system 620 in case the 1Phone data is lost on the mobile device 610.

[00102] The user may enable a proximity auto-lock feature for the data security system 620. During a communication session, the data security transceiver 624 of FIG. 6 reports to the data security system 620 a signal strength measurement for the mobile device 610. The data security system application 618 on the mobile device 610 sends the data security system 620 both the originating signal power level and the threshold for proximity.

[00103] Because the signal strength varies due to environmental conditions around the transceivers, the data security system 620 mathematically smooths the signal strength measurements to reduce the likelihood of a false positive. When the data security system 620 detects that the signal power received has dropped below a defined threshold for a predetermined period of time, it will immediately lock the data security system 620 and prevent access to the storage subsystem 106 of FIG. 6.

[00104] The data security system 620 could be used in three different modes: a User Mode where the functionalities of the data security system 620 are determined by the user; an Administrator Mode where an administrator can set an Administrator password and enforce some restrictions on the data security system 620 (e.g., automatic lock after a predetermined period of inactivity, Read-Only, 1Phone) and where restrictions cannot be removed by a User; and a Server Mode where an administrator role is set where the server/console 640 can remotely

reset the data security system 620, change user passwords, or just unlock the data security system 620.

[00105] Referring now to FIG. 8, therein is shown a unlocking sequence diagram where the mobile device 610 is an authentication factor. This diagram shows auto-unlock process of the data security system 620 initiated by the data security system application 618 from specific mobile device, the mobile device 610. A user can use only one mobile device that was initially paired with the data security system 620. If the paired mobile device 610 is lost then the data security system 620 could not be unlocked (unless administrator password was set before as shown in FIG. 7).

[00106] While similar to FIG. 7, a data security system application started operation 800 occurs after the connectivity 700 is established. An unlock required with mobile device ID signal 802 is sent from the mobile device 610 to the data security system 620 after a data security system connected, powered and discoverable operation 706. A data security system unlocked operation 804 occurs and a confirmation: data security system unlocked signal 712 is sent from the data security system 620. After a confirmation: data security system unlocked operation 806, the mobile device 610 and the data security system 620 are in full operative communication.

[00107] If a PIN (Personal Identification Number) was not setup then the paired mobile device is used as 1-authentication factor.

[00108] Referring now to FIG. 9, therein is shown an unlock sequencing diagram showing unlocking using a PIN entry from the mobile device 610. This diagram shows process of unlocking the data security system 620 by entering a PIN in the data security system application 618 in the mobile device 610. The data security system 620 cannot be unlocked without entering the correct PIN.

[00109] While similar to FIGs. 7 and 8, an enter username/password operation 900 occurs after the data security system application started operation 800. After the enter username/password operation 900, the mobile device 610 sends a verify user ID signal 902 to the server/console 640. The server/console 640 then makes a username/password valid determination 904.

[00110] When the username/password valid determination 904 verifies the user, a valid user signal 906 is sent to the mobile device 610 for the user to enter the correct PIN in an enter PIN operation 908 in the mobile device 610. The mobile device 610 then sends a verify unlock signal 910 to determine if the correct PIN has been entered to the server/console 640.

[00111] The server/console 640 makes a user authorized determination 912 and determines if the user is authorized to use the specific data security system, such as the data security system 620, that the PIN is authorized for. If authorized, an unlock allowed signal 914 is sent to the mobile device 610, which passes on an unlock request signal 916 to the data security system 620.

[00112] The data security system unlocked operation 804 is performed and the confirmation: data security system unlocked signal 712 is sent to the mobile device 610 where the confirmation: data security system unlocked operation 806 is performed.

[00113] Referring now to FIG. 10, therein is shown an unlock sequencing diagram showing unlock using a PIN entry and User ID/location/time verification via the server/console 640. This diagram shows the most secure process of unlocking the data security system 620 by entering a PIN in the data security system application 618 from the mobile device 610, authentication in the server/console 640 server using a UserID (username/password) and by verifying geo-fencing permissions to unlock the data security system 620 at a specific location and at a certain time range. The data security system 620 could not be unlocked without entering the PIN, username and password, and having the mobile device 610 be present in specific (predefined) location and certain (predefined) time.

[00114] While similar to FIGs. 7-9, at the server/console 640, an unlock specified data security system operation 1000 is performed to allow setting of the desired conditions under which the specified data security system, such as the data security system 620, will operate. For example, the conditions could be within a specific geographical area and/or specific time frame.

[00115] At the mobile device 610, a current condition determination is made, such as in an acquire location and/or current time operation 1002. This operation is performed to determine where the mobile device 610 is located and or what the current time is where the mobile device 610 is located. Other current conditions around the mobile device 610 may also be determined and sent by a verify unlock signal 1004 to the server/console 640 where a conditions met determination 1006 is made.

[00116] When the desired conditions are met, an unlock allowed signal 1008 is sent to the mobile device 610 for the enter PIN operation 908 to be performed. After the PIN is entered, a verify unlock signal 1010 is sent with the PIN and an identification of the data security system 620 that is in operational proximity to the mobile device 610. The verify unlock signal 1010 is received by the server/console 640 and a data security system allowed determination 1012 is

made to determine that the specified data security system is allowed to unlock by the authorized user. The server/console 640 verifies that this "specific" user is authorized to use the specified data security system.

[00117] After determining the correct information has been provided, the server/console 640 will provide an unlock allowed signal 914 to the mobile device 610, which will provide a unlock request signal 916. The unlock request signal 916 causes the data security system 620 to operate.

[00118] Referring now to FIG. 11, therein is shown a reset sequencing diagram showing resetting the data security system 620 using the server/console 640. This diagram shows the ability to reset the data security system 620 remotely via the server/console 640. The data security system 620 can receive commands only from the mobile device 610 over the wireless connection. However, by setting a "Reset" flag on the server/console 640 for a specific data security system (using it's S/N), the data security system application 618 running on the mobile device 610 will query the server/console 640 for any flags/pending requests in the user management database 642. When the user connects the data security system 620, the data security system application 618 on the mobile device 610 will execute a waiting "reset" command. After a successful reset (all user data and credentials are gone), the server/console 640 will remove the Reset flag so it will be not be executed the next time when the mobile device 610 is connected to the specific data security system.

[00119] While similar to FIGs. 7-10, the mobile device 610 responds to the valid user signal 906 to send an any command waiting signal 1100 to the server/console 640 to make a reset command determination 1102. When the reset command is present, a perform reset signal 1104 will be sent to the mobile device 610.

[00120] The mobile device 610 will send a reset security system signal 1106 to the data security system 620 to start a data security system reset operation 1108. Upon completion of the data security system reset operation 1108, the data security system 620 will send a confirmation: data security system reset signal 1110 to the mobile device 610 to set a confirmation: data security system reset operation 1112 into operation. Thereafter, the mobile device 610 and the data security system 620 are in full operative communication with the data security system 620 reset.

[00121] Referring now to FIG. 12, therein is shown an unlock sequencing diagram showing unlocking the data security system 620 using the server/console 640. This diagram shows ability to unlock the data security system 620 remotely via the server/console 640. The data

security system 620 can receive commands only from the mobile device 610 over the wireless connection. However by setting an "Administrator Unlock" flag on the server/console 640 console for a specific data security system (using it's S/N), the data security system application 618 running on the mobile device 610 will query the server/console 640 for any flags/pending requests. When the user connects the data security system 620, the data security system application 618 on the mobile device 610 will execute a waiting "Administrator Unlock" command. After successful Administrator unlock, the user's data is untouched, but the user's password is removed (the data security system 620 cannot be unlocked by the user). The server/console 640 will remove Reset flag for the data security system 620 so it will be not executed next time when the mobile device 610 is connected to the data security system 620.

[00122] While similar to FIGs. 7-11, after receiving the any command waiting signal 1100, the server/console 640 performs an unlock 1200 when there is a command to unlock with an administrator's password. An unlock with an administrator's password signal 1202 is sent to the mobile device 610, which provides an unlock with administrator's password signal 1204 to the data security system 620 to start the data security system unlocked operation 804. Thereafter, the mobile device 610 and the data security system 620 are in full operative communication.

[00123] Referring now to FIG. 13, therein is shown a change user's password sequencing diagram using the server/console 640. This diagram shows ability to change User's password for data security system 620 remotely via the server/console 640. Even data security system 620 can receive commands only from the mobile device 610 over the wireless connection, by setting a "Change User's Password" flag on the server/console 640 console for a specific data security system (using it's S/N), the data security system application 618 running on the mobile device 610 will query the server/console 640 for any flags/pending requests. When user will connect his data security system 620, the data security system application 618 on the mobile device 610 will execute waiting "Change User's Password" command. After successful unlock and changed password, the user's data is untouched and the data security system 620 can be unlocked with new user's password. The server/console 640 will remove "Change User's Password" flag for this data security system 620 so it will be not executed next time when the mobile device 610 is connected to the specific data security system.

[00124] While similar to FIGs. 7-12, the server/console 640 responds to the any command waiting signal 1100 by making a change password determination 1300. When there has been a password change at the server/console 640 a change user password signal 1302 is sent to the

mobile device 610, which sends a change user password signal 1304 to the data security system 620. Thereafter, the mobile device 610 and the data security system 620 are in full operative communication with the new password.

[00125] A method of operation of a data security system comprising: providing a mobile device with a data security system application for connectivity with the data security system; starting the data security system application; and maintaining connectivity of the data security system with the mobile device.

[00126] The method as described above wherein maintaining the connectivity maintains the connectivity when the data security system is within a predetermined proximity to the mobile device.

[00127] The method as described above wherein maintaining the connectivity maintains the connectivity when the data security system is within a predetermined proximity to the mobile device for a predetermined period of time.

[00128] The method as described above wherein establishing the connectivity includes using bi-directional communication between the data security system and the mobile device.

[00129] The method as described above wherein establishing the connectivity includes using uni-directional communication between the data security system and the mobile device.

[00130] The method as described above further comprising communication between the mobile device with the data security system application and a server containing a user management database.

[00131] The method as described above further comprising providing security information in a security controller in the data security system.

[00132] The method as described above further comprising: providing a server with identification of a specified data security system; providing the data security system with a specific identification; and unlocking the data security system when the identification of the specified data security system is the same as the specific identification of the data security system.

[00133] The method as described above wherein providing a mobile device with the data security system application provides a data security system administrator's application and further includes: setting an administrator's password in the mobile device; transmitting the administrator's password from the mobile device to the data security system; and setting the administrator's password in the data security system and unlocking the data security system.

[00134] The method as described above further comprising: providing an unlock request along with a mobile device identification from the mobile device to the data security system; and receiving the unlock request in the data security system and unlocking the data security system.

[00135] The method as described above further comprising: entering a user name or password in the mobile device; determining when the user name or password is valid in a server after receiving the user name or password from the mobile device; communicating from the server to the mobile device when the user name or password is valid; and communicating from the mobile device to the data security system when the user name or password is valid to unlock the data security system.

[00136] The method as described above further comprising: entering a user name or password in the mobile device; determining when the user name or password is valid in a server after receiving the user name or password from the mobile device; communicating from the server to the mobile device when the user name or password is valid; determining when the identification number is valid in the server after receiving identification number from the mobile device; and unlocking the data security system through the mobile device when the server determines the identification number is valid.

[00137] The method as described above further comprising: providing a valid location of the mobile device to a server; determining in the server when the mobile device is in the valid location; and unlocking the data security system through the mobile device when the server determines the mobile device is in the valid location.

[00138] The method as described above further comprising: providing a current time of operation for the data security system at the mobile device to a server; determining in the server when the mobile device is within the current time; and unlocking the data security system through the mobile device when the server determines the mobile device has the current time.

[00139] The method as described above further comprising: providing a command in a server; providing the command to the mobile device from the server in response to a command waiting signal from the mobile device; and performing the command in the data security system through the mobile device when the command is provided from the server.

[00140] The method as described above further comprising: providing a change password command in a server; providing the change password command to the mobile device from the server in response to a change password signal from the mobile device; and unlocking the data security system with the changed password in the data security system.

[00141] The method as described above further comprising connecting the data security system to a host computer for power and to be discoverable by the host computer.

[00142] A data security system comprising: a data security transceiver or receiver; an authentication subsystem operatively connected to the data security transceiver or receiver; and a storage subsystem connected to the authentication subsystem.

[00143] The system as described above further comprising a security controller connected to the data security transceiver or the receiver and to the authentication subsystem.

[00144] The system as described above further comprising a mobile device having a data security system application operating with the security controller for maintaining connectivity when the data security system is within a predetermined proximity to the mobile device.

[00145] The system as described above further comprising a mobile device having a data security system application operating with the security controller for maintaining connectivity when the data security system is within a predetermined proximity to the mobile device for a predetermined period of time.

[00146] The system as described above further comprising a mobile device having a mobile transceiver or receiver for maintaining connectivity includes using bi-directional communication between the data security system and the mobile device.

[00147] The system as described above further comprising a mobile device having a mobile transceiver or receiver for maintaining connectivity includes using uni-directional communication between the data security system and the mobile device.

[00148] The system as described above further comprising a wired or wireless connection communication between a mobile device with a data security system application and a server containing a user management database.

[00149] The system as described above wherein the data security system includes an external communication channel for connection to a host computer.

[00150] While the invention has been described in conjunction with a specific best mode, it is to be understood that many alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications, and variations that fall within the scope of the included claims. All matters set forth herein or shown in the accompanying drawings are to be interpreted in an illustrative and non-limiting sense.

CLAIMS

1. A method of operating a data security communication system including a mobile device, a remote server and a portable memory device, the portable memory device comprising an interface controller for communications through a data channel, a storage medium, an authentication subsystem having an authentication key and an encryption key, an encryption engine, and a wireless transceiver for radiofrequency communications outside the data channel, the portable memory device being locked when the storage medium is not accessible via the data channel and unlocked when the storage medium is accessible via the data channel, the method comprising:

establishing a connection with the mobile device;

receiving user authentication input, via the wireless transceiver from the mobile device, while the portable memory device is locked, wherein the mobile device includes a user interface for receiving user information, the mobile device being configured for interacting with the remote server to validate the user information and for generating the user authentication input for unlocking the portable memory device, wherein the user authentication input is received by the portable memory device after the user information is validated by the remote server;

unlocking the portable memory device based on the received user authentication input and the authentication key of the authentication subsystem; and

while the portable memory device is unlocked:

encrypting, with the encryption key, data received through the data channel before storing the encrypted data in the storage medium; and

decrypting, with the encryption key, data read from the storage medium before sending the decrypted data through the data channel.

2. The method as recited in claim 1, further comprising:

transmitting the encryption key from the authentication subsystem to the encryption engine based on the unlocking, wherein the encryption key is not stored in the storage medium of the portable memory device, wherein the encryption key is not accessible from an outside of the portable memory device.

3. The method as recited in claim 1, wherein receiving the user authentication

20 17 06

input further comprises:

communicating with an application in the mobile device via the wireless transceiver; and

receiving the user authentication input from the mobile device.

4. The method as recited in claim 3, further comprising:

receiving a command to change the authentication key from the application in the mobile device after the application in the mobile device receives the command to change the authentication key from the remote server.

5. The method as recited in claim 1, wherein an application in the mobile device allows the mobile device to lock the portable memory device, unlock the portable memory device, change a user name, change the authentication key, and reset the portable memory device.

6. The method as recited in claim 1, wherein an application in the mobile device enables the remote server to reset the portable memory device and to unlock the portable memory device.

7. The method as recited in claim 1, wherein an application in the mobile device enables the remote server to restrict use of the portable memory device to specific locations using geo-fencing by determining presence of the mobile device within the geo-fence.

8. The method as recited in claim 1, wherein an application in the mobile device enables the remote server to restrict use of the portable memory device to specific time zones and time periods.

9. The method as recited in claim 1, wherein the data channel is a computer bus channel.

10. The method as recited in claim 1, wherein the radiofrequency communications includes one of Wireless Fidelity (WiFi), Bluetooth (BT), Bluetooth Smart (BLE), Near Field Communication (NFC), or cellular communication.

11. A data security communication system including:

a mobile device, a remote server and a portable memory device, the portable memory device comprising:

an interface controller for communications through a data channel;

a storage medium, the portable memory device being locked when the storage medium is not accessible via the data channel and unlocked when the storage medium is accessible via the data channel;

a wireless transceiver for radiofrequency communications outside the data channel, the wireless transceiver being configured for establishing a connection with the mobile device and receiving user authentication input from the mobile device, wherein the mobile device includes a user interface for receiving user information, the mobile device being configured for interacting with the remote server to validate the user information and for generating the user authentication input for unlocking the portable storage device, wherein the user authentication input is received from the mobile device after the user information is validated by the remote server;

an authentication subsystem having an authentication key and an encryption key, the authentication subsystem unlocking the portable memory device based on the received user authentication input and the authentication key; and

an encryption engine for encrypting, with the encryption key, data received through the data channel before storing the encrypted data in the storage medium, and for decrypting, with the encryption key, data read from the storage medium before sending the decrypted data through the data channel.

12. The data security communication system as recited in claim 11, wherein the authentication subsystem transmits the encryption key to the encryption engine based on the unlocking, wherein the encryption key is not stored in the storage medium of the portable memory device, wherein the encryption key is not accessible from the outside of the portable memory device.

13. The data security communication system as recited in claim 11, wherein receiving the user authentication input further comprises:

communicating with an application in the mobile device via the wireless transceiver; and

receiving, via the wireless transceiver, the user authentication input from the mobile device.

14. The data security communication system as recited in claim 13, wherein the authentication subsystem is configured for receiving a command to change the authentication key from the application in the mobile device after the application in the mobile device receives the command to change the authentication key from the remote server.

15. A machine-readable storage medium carrying instructions that, when executed by a plurality of machines, cause the machines to perform the method of any one of claims 1 to 10.

20 17 0690