



- (51) **International Patent Classification:**
G06F 12/16 (2006.01) *G06F 13/14* (2006.01)
- (21) **International Application Number:**
PCT/US2013/040355
- (22) **International Filing Date:**
9 May 2013 (09.05.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/651,670 15 October 2012 (15.10.2012) US
- (71) **Applicant:** DELL PRODUCTS L.P. [US/US]; One Dell Way, Round Rock, TX 78682-2244 (US).
- (72) **Inventors:** O'CONNOR, Clint, H.; 12501 Tech Ridge Blvd., Apt. 1812, Austin, TX 78753 (US). ENDERS, Kevin; 708 Tofino Cove, Round Rock, TX 78665 (US). HAZE, Michael; 4004 Mayfield Cove Trail, Round Rock, TX 78681 (US). ANDREWS, Carlton; 6308 Mauna Kea Drive, Austin, TX 78746 (US).
- (74) **Agent:** PREWITT, Brian, K.; Jackson Walker, L.L.P., 100 Congress Avenue, Suite 1100, Austin, TX 78701 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) **Title:** SYSTEM AND METHOD FOR MIGRATION OF DIGITAL ASSETS LEVERAGING DATA PROTECTION

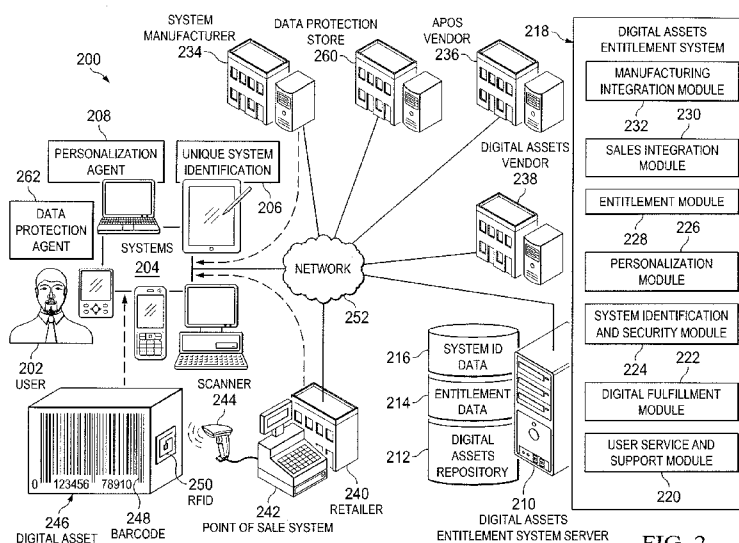


FIG. 2

(57) **Abstract:** In accordance with embodiments of the present disclosure, an information handling system may include a storage medium and a processor. The storage medium may be configured to store data comprising backup data associated with a source system. The processor may be configured to migrate the data from the storage medium to a target system. The processor may further be configured to during migration of the data from the storage medium to the target system, receive additional data comprising additional backup data associated with the source system and store the additional data to the storage medium. The processor may also be configured to migrate the additional data to the target system.

**SYSTEM AND METHOD FOR MIGRATION OF DIGITAL ASSETS LEVERAGING
DATA PROTECTION**

TECHNICAL FIELD

The present disclosure relates to the management of
5 information handling systems. More specifically, embodiments
of the disclosure provide a system, method, and article of
manufacture for migrating digital assets from a source
system to a target system.

BACKGROUND

As the value and use of information continues to increase, individuals and businesses seek additional ways to process and store information. One option available to users is information handling systems. An information handling system generally processes, compiles, stores, and/or communicates information or data for business, personal, or other purposes thereby allowing users to take advantage of the value of the information. Because technology and information handling needs and requirements vary between different users or applications, information handling systems may also vary regarding what information is handled, how the information is handled, how much information is processed, stored, or communicated, and how quickly and efficiently the information may be processed, stored, or communicated. The variations in information handling systems allow for information handling systems to be general or configured for a specific user or specific use such as financial transaction processing, airline reservations, enterprise data storage, or global communications. In addition, information handling systems may include a variety of hardware and software components that may be configured to process, store, and communicate information and may include one or more computer systems, data storage systems, and networking systems.

In recent years, it has become common for manufacturers to offer purchasers the ability to order a system custom-configured to purchaser specification. These custom-configured systems, which are often ordered online, allow the purchaser to select the operating system (OS) of their choice along with a selection of software and other digital assets to meet their individual needs. In some cases, the

manufacturer may preinstall the OS and the selected digital assets on the system prior to delivery. In addition, the system may be further personalized (e.g., desktop themes and colors, etc.) as a service to the customer. Such

5 customizations and personalizations may be limited only by the customer's patience and willingness to define or describe their ideal system.

However, there is currently no easy way for the purchaser to migrate software and other digital assets from an existing system to a newly purchased system. As a result, the customer has to locate the original distribution media and license keys that came with the existing system or were purchased later. In the event of downloaded digital assets, the purchaser typically has to find back-up copies of the original downloaded files and emails that include the associated license keys. If they are not located, or if they were lost due to a system failure such as, for example, a crashed hard drive, the purchaser has to log-on to the digital assets provider site, download the files again, and then perform an authentication routine to receive the license keys via email. Moreover, it is not uncommon for users to misplace or forget their User IDs and passwords. While methods exist to recover a log-in name and password, the process is inherently cumbersome, which may further delay the user's recovery of the digital assets. As a result, these issues may either lengthen the time required to replace an existing system or cause system owners to consider alternatives, such as thin client approaches (e.g., netbooks), cloud-based computing, or alternative operating systems. In view of the foregoing, there is a need for more easily migrating digital assets from an existing system to a

10
15
20
25
30

new system without requiring the user to provide installation files and associated license keys.

Further complicating migrations of software and other digital assets from a source system to a target system is
5 the fact that the volume of data represented by migrated digital assets may be large, thereby requiring a significant amount of time for migrations to complete, which may negatively affect user experience.

SUMMARY

In accordance with the teachings of the present disclosure, the disadvantages and problems associated with migration of digital assets have been substantially reduced or eliminated.

In accordance with embodiments of the present disclosure, an information handling system may include a storage medium and a processor. The storage medium may be configured to store data comprising backup data associated with a source system. The processor may be configured to migrate the data from the storage medium to a target system. The processor may further be configured to during migration of the data from the storage medium to the target system, receive additional data comprising additional backup data associated with the source system and store the additional data to the storage medium. The processor may also be configured to migrate the additional data to the target system.

In accordance with these and other embodiments of the present disclosure, a computer-implemented method for migrating digital assets may include migrating, from a storage medium configured to store data comprising backup data associated with a source system, the data to a target system. The method may also include while migrating the data from the storage medium to the target system, receiving additional data comprising additional backup data associated with the source system and storing the additional data to the storage medium. The method may further include migrating the additional data to the target system from the storage medium.

In accordance with these and other embodiments of the present disclosure, an article of manufacture may include a

computer readable medium and computer-executable instructions carried on the computer readable medium. The instructions may be readable by a processor, the instructions, when read and executed, for causing the processor to: (i) migrate, from a storage medium configured to store data comprising backup data associated with a source system, the data to a target system; (ii) while migrating the data from the storage medium to the target system, receive additional data comprising additional backup data associated with the source system and store the additional data to the storage medium; and (iii) migrate the additional data to the target system from the storage medium.

Technical advantages of the present disclosure may be apparent to those of ordinary skill in the art in view of the following specification, claims, and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present embodiments and advantages thereof may be acquired by referring to the following description taken in conjunction
5 with the accompanying drawings, in which like reference numbers indicate like features, and wherein:

FIGURE 1 illustrates a block diagram of an example information handling system, in accordance with embodiments of the present disclosure;

10 FIGURE 2 illustrates a block diagram of an example digital assets entitlement system in accordance with components of the present disclosure;

FIGURES 3A-B illustrate block diagrams of an example unique system identifier that remains the same when one of
15 its associated system component identifiers has been changed, in accordance with embodiments of the present disclosure;

FIGURES 4A-B illustrate block diagrams of an example unique system identifier that is changed when one of its
20 associated system component identifiers has been changed, in accordance with embodiments of the present disclosure;

FIGURE 5 illustrates a block diagram of an example encrypted unique system identifier generated from a set of system component identifiers, in accordance with embodiments
25 of the present disclosure;

FIGURE 6 illustrates a block diagram of an example unique system identifier decrypted from an encrypted unique system identifier, in accordance with embodiments of the present disclosure;

30 FIGURES 7A-B illustrate a flow chart of an example method for performance of digital asset entitlement

operations, in accordance with embodiments of the present disclosure;

FIGURE 8 illustrates a flow chart of an example method for performance of digital assets migration operations, in accordance with embodiments of the present disclosure; and

FIGURE 9 illustrates a flow chart of an example method for migrating digital assets between a target system and a cloud storage provider, in accordance with embodiments of the present disclosure.

DETAILED DESCRIPTION

Preferred embodiments and their advantages are best understood by reference to FIGURES 1-9, wherein like numbers are used to indicate like and corresponding parts.

5 For the purposes of this disclosure, an information handling system may include any instrumentality or aggregate of instrumentalities operable to compute, classify, process, transmit, receive, retrieve, originate, switch, store, display, manifest, detect, record, reproduce, handle, or
10 utilize any form of information, intelligence, or data for business, scientific, control, entertainment, or other purposes. For example, an information handling system may be a personal computer, a personal digital assistant (PDA), a consumer electronic device, a network storage device, or
15 any other suitable device and may vary in size, shape, performance, functionality, and price. The information handling system may include memory, one or more processing resources such as a central processing unit (CPU) or hardware or software control logic. Additional components
20 of the information handling system may include one or more storage devices, one or more communications ports for communicating with external devices as well as various input and output (I/O) devices, such as a keyboard, a mouse, and a video display. The information handling system may also
25 include one or more buses operable to transmit communication between the various hardware components.

FIGURE 1 illustrates a block diagram of an example information handling system 100, in accordance with
embodiments of the present disclosure. Information handling
30 system 100 may include a processor 102, I/O devices 104, a hard drive or disk storage 106, a network port 110, a memory 112, various other information handling resources 108, all

communicatively coupled to each other via one or more buses 114. In some embodiments an information handling system identification similar to that depicted in FIGURE 1 may be used to implement one or more methods and/or systems disclosed herein.

A processor 102 may include any system, device, or apparatus configured to interpret and/or execute program instructions and/or process data, and may include, without limitation a microprocessor, microcontroller, digital signal processor (DSP), application specific integrated circuit (ASIC), or any other digital or analog circuitry configured to interpret and/or execute program instructions and/or process data. In some embodiments, processor 102 may interpret and/or execute program instructions and/or process data stored in memory 112, hard drive 106, and/or another component of system 100.

An I/O device 104 may include any system, device, or apparatus from which processor 102 may receive input or to which processor 102 may deliver output. An I/O device may include a display, a keyboard, a mouse, other I/O devices, and/or associated controllers.

Hard drive 106 may include computer-readable media (e.g., magnetic storage media, optical storage media, opto-magnetic storage media, and/or other type of rotating storage media, flash memory, and/or other type of solid state storage media) and may be generally operable to store data and/or programs (e.g., one or more operating systems and/or one or more application programs). Although FIGURE 1 depicts information handling system 100 as including one hard drive 106, information handling system 100 may include any suitable number of hard drives 106.

Network port 110 may include any suitable system, apparatus, or device operable to serve as an interface between information handling system 100 and a network. Network port 110 may enable information handling system 102 to communicate over such network using any suitable transmission protocol and/or standard, including without limitation Fibre Channel, Frame Relay, Asynchronous Transfer Mode (ATM), Internet Protocol (IP), other packet-based protocol, small computer system interface (SCSI), Internet SCSI (iSCSI), Serial Attached SCSI (SAS) or any other transport that operates with the SCSI protocol, advanced technology attachment (ATA), serial ATA (SATA), advanced technology attachment packet interface (ATAPI), serial storage architecture (SSA), integrated drive electronics (IDE), and/or any combination thereof.

Memory 112 may be communicatively coupled to processor 102 and may include any system, device, or apparatus configured to retain program instructions and/or data for a period of time (e.g., computer-readable media). Memory 112 may include random access memory (RAM), electrically erasable programmable read-only memory (EEPROM), a Personal Computer Memory Card International Association (PCMCIA) card, flash memory, magnetic storage, opto-magnetic storage, or any suitable selection and/or array of volatile or non-volatile memory that retains data after power to information handling system 100 is turned off. Although FIGURE 1 depicts information handling system 100 as including one memory 112, information handling system 100 may include any suitable number of memories 112.

Other information handling resources 108 may include any component systems, devices, or apparatuses of an information handling system 100, including without

limitation processors, buses, memories, I/O devices and/or interfaces, storage resources, network interfaces, motherboards, electro-mechanical devices (e.g., fans), displays, and power supplies.

5 The one or more buses 114 may comprise any suitable collection of systems, devices, or apparatuses configured to transfer data between various components of information handling system 100. For example, one or more buses 114 may include a serial advanced technology attachment (SATA) bus,
10 a Peripheral Component Interconnect (PCI)/PCMCIA bus, Universal Serial Bus (USB), an SCSI bus, FireWire (IEEE 1394) bus, InfiniBand bus, any other suitable bus, or any combination of the foregoing.

FIGURE 2 illustrates a block diagram of an example
15 digital assets entitlement system 218, in accordance with embodiments of the present disclosure. In some embodiments, digital assets entitlement system 218 may be implemented for managing the entitlement of a system 204 to process a digital asset 246. In these and other embodiments, digital
20 assets entitlement system 218 may be implemented on one or more servers 210, which may be commercially coupled to a network 252. In various embodiments, network 252 may comprise a public network, for example the Internet, a physical private network, a virtual private network (VPN),
25 or any combination thereof. As shown in FIGURE 2, digital assets entitlement system 218 may include a user service and support module 220, a digital fulfillment module 222, and a system identification and security module 224. Digital assets entitlement system 218 may likewise comprise a
30 personalization module 226, an entitlement module 228, a sales integration module 230, and a manufacturing integration module 232. In addition, digital assets

entitlement system 218 may be configured to access a digital assets data repository 212, an entitlement data repository 214, and a system identifier (ID) data repository 216, each of which may be implemented on one or more servers 210

5 communicatively coupled to a network 252.

As used herein, a digital asset 246 refers to any digital asset, for example, a software application, a deliverable or performable service, music, video, software activation key, personalization instructions, files, etc.
10 that are digitally deliverable either wholly or partially. As likewise used herein, a digital assets entitlement may refer to the association of a predetermined digital asset 246 with a target system 204. In various embodiments, an entitlement record may include the digital assets
15 entitlement data (e.g., license information, etc.) that allows digital asset 246 to be processed by a target system 204 identified by a corresponding unique system identifier 206. In these and other embodiments, the entitlement record may be processed by entitlement module 228 and stored in
20 entitlement data repository 214. Likewise, as used herein, a system 204 may comprise an information handling system (e.g., a personal computer, a laptop computer, a tablet computer, a PDA, a mobile telephone, or any other suitable device) operable to store a unique system ID 206, perform
25 digital asset entitlement operations with a personalization agent, and operable to establish an online session with digital assets entitlement system 218 via network 252.

In some embodiments, digital assets entitlement and system personalization operations may be performed by a user
30 202, in either a physical environment or an online environment. A user 202 may comprise a system purchaser enterprise administrator, information technologist, or

another suitable person. As an example, a physical environment may comprise a retailer 240 operating a physical point-of-sale (POS) system 242. As another example, an online environment may comprise a system manufacturer 234, after-point-of-sale (APOS) vendor 236, or digital assets vendor 238, that respectively accepts online orders for systems or digital assets via network 252.

If the digital assets entitlement and system personalization operations are performed in an online environment, then user 202 may decide whether to purchase a custom-configured or pre-configured system 204. If the system 204 is to be pre-configured, then it may be selected for online purchase by the user 202 and its unique identifier 206 may be determined. In some embodiments, the unique system identifier 206 may be stored in the basic input/output system (BIOS) of the pre-configured system 204. However, if the system 204 is to be custom-configured, then it may be custom-configured for online purchase by user 202. Once manufactured by system manufacturer 234, a unique system identifier may be generated as described in greater detail herein.

In various embodiments, manufacturing integration module 232 may coordinate the custom configuration of the system 204 with digital assets entitlement system 218. Likewise, system identification and security module 224 may coordinate the generation of unique system identifier 204 and its storage in the repository of system identifier data 216. User 202 may then select a digital asset 246 for online purchase, followed by selecting personalization options for the pre-configured or custom-configured system 209. In various embodiments, the personalization module 226 coordinates the selection of personalization options with

digital assets entitlement system 218. As used herein, a system personalization option refers to any feature, capability, or function that may be applied to a target system 204. As an example, a personal computer desktop wallpaper or user interface options (e.g., a "classic" interface) are personalization options.

However, if the digital assets entitlement and system personalization operations are performed in a physical environment, then user 202 may select a pre-configured system 204 and physical representations of digital assets 246 to be purchased. In various embodiments, the digital asset 246 may be physically represented as images and/or text on a card or a package, yet the digital assets themselves may not be included within the card or package. User 202 may then select system personalization options for the pre-configured system 204. In various embodiments, the system personalization options may likewise be physically represented as images and/or text on a card or a package.

The digital assets product identifier (ID) may then be scanned with a scanner 244 from its corresponding physical representation, followed by scanning its corresponding digital assets activation key or other entitlement data. In various embodiments, it is not necessary to scan the digital assets activation key or other entitlement data as it is provided by digital assets entitlement system 218 during digital asset entitlement operations described in greater detail herein. Data related to the previously selected personalization options may then likewise be scanned, followed by determining unique system identifier 206 of pre-configured system 204. In various embodiments, the digital assets product ID, its associated activation key or entitlement data, the personalization option data, and the

unique system identifier may be represented by a bar code
248 or other indicia on a card or physical package. In
various other embodiments, the digital assets product ID,
its associated activation key or entitlement data, the
5 personalization option data, and the unique system
identifier may be stored in a radio frequency identifier
(RFID) 250 tag affixed to the physical representation of the
digital asset. Those of skill in the art may appreciate that
many such embodiments are possible and that the foregoing is
10 not intended to limit the spirit, scope, or intent of the
disclosure.

A purchase transaction for the custom-configured or
pre-configured system 204 and any associated digital assets
246 and personalization options may then be completed. In
15 various embodiments, the processing of the purchase
transaction may be performed by the sales integration module
230. In these and other embodiments, the financial proceeds
of the purchase transaction may be settled between multiple
parties. For example, a system manufacturer 234 may receive
20 a portion of the purchase transaction corresponding to the
cost of the system 204. One or more digital assets vendors
238 may likewise receive a proportionate share of the
purchase transaction corresponding to the digital asset 246
they respectively provide.

25 Digital asset entitlement operations, as described in
greater detail herein, may then be performed by digital
assets entitlement system 218 to bind the digital assets
246, the personalization options, and their respective
digital assets entitlement data to unique system identifier
30 206 of target system 204. The resulting bound data,
including data associated with the digital assets (e.g.,
installation files, etc.) may then be stored in the

repository of entitlement data 214 and purchased system 204 may then be delivered to user 202 or another person designated by user 202. In various embodiments, entitlement module 228 may generate, and then process, the digital
5 assets entitlement data and user service and support module 220 may coordinate the delivery of system 204 to user 202 or another person designated by user 202.

Standard operating system (OS) out-of-the-box-experience (OOBE) or hypervisor boot operations may be
10 performed on the system 204, followed by loading a personalization agent 208. In various embodiments, the personalization agent 208 has a unique identifier that may be associated with one or more unique system component identifiers. In some embodiments, the unique identifier of
15 the personalization agent may be uniquely associated with the current unique system identifier 206 associated with the system 204. In other embodiments, a portion of the personalization agent 208 may be delivered to the system 204 in an encrypted form and may then be decrypted prior to
20 being loaded on the system 204. In these embodiments, the primary system identifier (e.g., service tag number, serial number, etc.), may be used as a decryption key to decrypt the personalization agent 208.

In these and other embodiments, secondary system
25 identifiers may be stored on system 204 (e.g., in the BIOS, in flash memory, on a hard disk, etc.) as well as in digital assets entitlement system 218. In these and other embodiments, digital assets entitlement system 218 may use the secondary system identifiers to encrypt a portion of
30 personalization agent 208 before it is downloaded to system 204. Once downloaded, the unencrypted portion of personalization agent 208 may use the secondary system

identifiers stored on system 204 to decrypt the encrypted portion of personalization agent 208. In some embodiments, the secondary system identifiers may likewise be encrypted and may first be decrypted before they are used to decrypt the encrypted portion of personalization agent 208. In other 5 embodiments, the secondary system identifiers may be stored in a Trusted Platform Module (TPM). Skilled practitioners of the art may appreciate that many such embodiments are possible and the foregoing is not intended to limit the spirit, scope, or intent of the disclosure. 10

Personalization agent 208 may query target system 204 for its unique system identifier 206. In various embodiments, unique system identifier 206 associated with system 204 may be stored in the target system's BIOS, flash 15 memory, a hard disk, and/or other memory device. Personalization agent 208 may then automatically establish a communication session with digital assets entitlement system 218 and use unique system identifier 206 to authenticate system 204. Unique system identifier 206 may then be used by 20 the personalization agent 208 to determine entitled digital assets and personalization options corresponding to the unique system identifier 206.

Once determined, the corresponding personalization options and digital assets 246, along with their associated 25 digital assets entitlement data, may be respectively downloaded to target system 204 from the repository of digital assets 212 and the repository of entitlement data 214. In some embodiments, the personalization options and digital assets 246, along with their associated digital 30 assets entitlement data 214, may be downloaded from a single server 210 on network 252. In other embodiments, the personalization options and digital assets 246 may be

downloaded from one or more servers 210 on network 252. In yet other embodiments, the personalization options, digital assets 246, and associated digital assets entitlement data 214 may be respectively downloaded from a plurality of servers 210 on network 252. As an example, a first digital asset 246 may be provided by system manufacturer 234 and a second digital asset 246 may be provided by a digital assets vendor 238. Likewise, a plurality of digital assets 246 may be provided by a corresponding plurality of digital assets vendors 238. Skilled practitioners of the art may appreciate that many such embodiments and examples are possible and the foregoing is not intended to limit the spirit, scope, or intent of the disclosure.

In various embodiments, digital assets entitlement system 218 may manage the respective location of the personalization options, digital assets 246, and associated digital assets entitlement data 214 to initiate its provision. Once downloaded, personalization agent 208 may use digital assets entitlement data 214 to install digital assets 246 and personalization options on system 204. Thereafter, user 202 or another person may decide to perform an APOS purchase of digital asset 246. As used herein, an APOS purchase of digital assets may refer to any purchase of digital asset 246 made after the initial online or physical purchase of system 204. In various embodiments, the APOS purchase of a digital asset 246 may be performed in a physical, online, or enterprise point-of-sale environment. If the APOS purchase is performed in an online environment, for example from APOS vendor 236, then user 202 or another person may select a digital asset 246 for online purchase. Personalization agent 208 may then determine unique system identifier 206 of system 204. An APOS purchase transaction

may then be performed for purchase of the selected digital asset 246. However, if the APOS purchase is performed in a physical environment, then the user 202 or another person may select a physical representation of a digital asset 246 to be purchased. The digital assets product ID may then be scanned from its corresponding physical representation, followed by scanning its corresponding digital assets activation key or other entitlement data.

Digital asset entitlement operations, as described in greater detail herein, may then be performed by digital assets entitlement system 218 to bind digital assets 246 and their respective digital assets entitlement data 214 associated with the APOS purchase to unique system identifier 206 of target system 204. The resulting bound data, including data associated with the digital assets (e.g., installation files, etc.) may then be stored, as described in greater detail herein, in digital assets entitlement system 218. Personalization agent 208, as likewise described in greater detail herein, then automatically establishes a communicative session with digital assets entitlement system 218, and may download the purchased digital assets 246 and their associated digital assets entitlement data 214. Once downloaded, personalization agent 208 may then use the associated digital assets entitlement data 214 to install the downloaded digital asset 246 on system 204.

A system 204 may also be configured to perform data protection. Data protection (which may also be known as "continuous data protection") refers to a backup of computer data stored on a system by automatically saving, either continuously or at regular intervals, a copy of changes made to such data, thereby capturing versions of the data saved

by a user. In some embodiments of data protection, data protection is accomplished by a series of periodical snapshots of data taken at regular intervals, wherein each snapshot represents changes made to the data since the
5 previous snapshot. Thus, data protection may allow a user or administrator of a system to restore data to a previous point in time by appropriately "rolling back" snapshots.

To accomplish data protection, a system 204 may execute a data protection agent 262. A data protection agent 262
10 may comprise a program of instructions stored on a computer-readable medium associated with a system 204, and executable on such system 204. In operation, the data protection agent 262 may, at specified intervals, generate a snapshot of data present on the system 204, wherein each snapshot represents
15 the changes or "delta" from the previously-generated snapshot. Once a snapshot has been generated, the data protection agent 262 may communicate the snapshot via network 252 to a data protection store 260 remote from the system 204. Accordingly, if a failure occurs at system 204,
20 the snapshots stored on the data protection store 260 may be used to restore data on the system 204 (or a replacement system 204) to a previous state.

FIGURES 3A-B illustrate a block diagram of an example unique system identifier 320 that remains the same when one
25 of its associated system component identifiers has been changed; in accordance with embodiments of the present disclosure. As shown in FIGURE 3A, an original unique system identifier 320 may be generated from a plurality of unique system component identifiers 302, which correspond to a
30 plurality of system components included in a target system 204. As likewise shown in FIGURE 3A, unique system component identifiers 302 may comprise a Model Number 304 `SA310J43`,

a Serial Number 306, sometimes referred to as a service tag number or a primary system identifier, `SEM5239923875`, a Factory ID 308 `AUS`, and a Manufacture Date 310 `111909`. Unique system component identifiers 302 may likewise
5 comprise an Original Motherboard ID 314 `19374WS238017BH`, a Processor ID 316 `92348430-432919237`, a Hard Drive ID 318 `L83747HJ3672`, etc.

As described in greater detail herein, once generated, original unique system identifier 320 may be associated,
10 such as, for example, through a binding operation, with predetermined digital assets 332 to generate a digital assets entitlement 330. As likewise described in greater detail herein, digital assets entitlement 330 entitle a target system 204, which may be associated with the original
15 unique system identifier 320, to process the digital assets 332. However, it is not uncommon for system components to be replaced due to failure, erratic performance, becoming outmoded, or for other reasons. It will be appreciated that the entitlement 330 between original unique system
20 identifier 320 and digital assets 332 may be compromised as a result of such a replacement. For example, as illustrated in FIGURE 3B, the Original Motherboard ID 314 `19374WS238017BH` may be replaced with a New Motherboard ID 334 `56812FR853945PL`. However, in such case the original
25 unique system identifier 320 may remain unchanged.

In various embodiments, extract, transform, and load (ETL) and other database operations may be performed to manage the integrity of the relationship between original unique system identifier 320 and the plurality of unique
30 system component identifiers 302. As an example, Original Motherboard ID 314 `19374WS238017BH` may remain as a subset of original unique system identifier 320, even though it may

have been deactivated or invalidated as a unique system component identifier 302. However, in these and other embodiments, relational database operations known to those of skill in the art may be applied to maintain the relationship between original unique system identifier 320, New Original Motherboard ID 334 `56812FR853945PL`, and unchanged unique system component identifiers 302. Accordingly, the integrity of entitlement 330 between original unique system identifier 320 and digital assets 332 may be perpetuated. It may be appreciated by skilled practitioners of the art that many such embodiments are possible and the foregoing is not intended to limit the spirit, scope, or intent of the disclosure.

FIGURES 4A-B illustrate a block diagram of an example unique system identifier 320 that is changed when one of its associated system component identifiers has been changed, in accordance with embodiments of the present disclosure. As shown in FIGURE 4A, an original unique system identifier 320 may be generated from a plurality of unique system component identifiers 302, which correspond to a plurality of system components included in a target system 204. As likewise shown in FIGURE 3A, unique system component identifiers 302 may comprise Model Number 304 `SA310J43`, Serial Number 306, sometimes referred to as a service tag number or a primary system identifier, `SEM5239923875`, Factory ID 308 `AUS`, and Manufacture Date 310 `111909`. Unique system component identifiers 302 may likewise comprise Original Motherboard ID 314 `19374WS238017BH`, Processor ID 316 `92348430-432919237`, Hard Drive ID 318 183747HJ3672', etc.

As described in greater detail herein, once generated, original unique system identifier 320 may be associated, such as, for example, through a binding operation, with

predetermined digital assets 332 to generate a digital assets entitlement 330. As likewise described in greater detail herein, digital assets entitlement 330 entitles a target system 204, which may be associated with original unique system identifier 320, to process digital assets 332. However, it is not uncommon for system components to be replaced due to failure, erratic performance, becoming outmoded, or for other reasons. It will be appreciated that entitlement 330 between the original unique system identifier 320 and digital assets 332 may be compromised as a result of such a replacement. For example, as illustrated in FIGURE 4B, Original Motherboard ID 314 `19374WS238017BH` may be replaced with New Motherboard ID 334 `56812FR853945PL`. As result, a new unique system identifier 420 may be generated, which may be a concatenation of the plurality of unique system component identifiers 402, including New Original Motherboard ID 334 `56812FR853945PL` as a subset.

In various embodiments, a first set of operations may be performed to remove entitlement 330 between original unique system identifier 320 and digital assets 332. A second set of operations may then be performed to associate new unique system identifier 420 with digital assets 332 to generate a new entitlement 430. In these and other embodiments, original unique system identifier 320 may then be invalidated. Accordingly, the integrity of original entitlement 330 between original unique system identifier 320 and digital assets 332 may be perpetuated by new entitlement 430 between new unique system identifier 420 and digital assets 332. Skilled practitioners of the art may appreciate that many such embodiments are possible and the

foregoing is not intended to limit the spirit, scope, or intent of the disclosure.

FIGURE 5 illustrates a block diagram of an example encrypted unique system identifier 528 generated from a set of system component identifiers, in accordance with embodiments of the present disclosure. In these embodiments, a source unique system identifier 520 may be generated from a plurality of original unique system component identifiers 502, which may correspond to a plurality of system components included in a target system 204. As shown in FIGURE 5, original unique system component identifiers 502 may comprise Model Number 304 `SA310J43`, Serial Number 306, sometimes referred to as a service tag number or a primary system identifier, `SEM5239923875`, Factory ID 308 `AUS`, Timestamp Date 510 `111909`, and Timestamp Time 512 `14:27:26:34`. Original unique system component identifiers 502 may likewise comprise Original Motherboard ID 314 `19374WS238017BH`, Processor ID 316 `92348430-432919237`, Hard Drive ID 318 183747HJ3672', etc.

An encryption operation 524 may then be performed on source unique system identifier 520 to generate original encrypted unique system identifier 528. In various embodiments, the encryption operation may comprise the use of a private key, a public key, key pairs, or any combination of keys and cryptographic operations such as implemented in a public key infrastructure (PKI), for example. As an example, the original encrypted unique system identifier 528 may be generated using a private key associated with the manufacturer of the system and a public key associated with the system itself. In some embodiments, the Timestamp Date 510 `111909` and the Timestamp Time 512 `14:27:26:34` may likewise be used to generate the encrypted

unique system identifier 528. Skilled practitioners of the art may be familiar with such cryptographic operations and may appreciate that many such embodiments are possible and that the foregoing is not intended to limit the spirit,
5 scope, or intent of the disclosure.

As described in greater detail herein, once generated, original encrypted unique system identifier 528 may be associated, such as, for example, through a binding operation, with predetermined digital assets 332 to generate
10 a digital assets entitlement 530. As likewise described in greater detail herein, digital assets entitlement 530 may entitle a target system 204, which may be associated with original encrypted unique system identifier 528, to process digital assets 332.

15 FIGURE 6 illustrates a block diagram of an example unique system identifier decrypted from an encrypted unique system identifier 622, in accordance with embodiments of the present disclosure. It is not uncommon for system components to be replaced due to failure, erratic performance, becoming
20 outmoded, or for other reasons. However, the replaced system component will typically have a different unique system component identifier. As a result, the entitlement association between a unique system identifier and predetermined digital assets may be compromised as a result
25 of such a replacement, which in turn may prevent target system 204 from processing the digital assets 246.

In various embodiments, the unique system component identifier of the replacement system component may be unknown until it is replaced in the target system 204. In
30 these and other embodiments, the system component may be replaced in the target system 204, the target system may then be initiated (e.g., booted), and an inventory of unique

system component identifiers may be performed. In some embodiments, one or more unique system component identifiers, for example a serial number or service tag, may be visible and may be visually inventoried. In other
5 embodiments, one or more unique system component identifiers, for example a motherboard, processor, or hard drive serial number, may not be visible and may be automatically inventoried.

As shown in FIGURE 6, a new source unique system
10 identifier 650 may be generated from the inventoried unique system component identifiers. In some embodiments, a time stamp date and a time stamp time may be components of new source unique system identifier 650. In these embodiments, the time stamp date and a time stamp time may be used to
15 validate the authenticity of new source unique system identifier 650. As an example, the provider of the replacement part may have stipulated that the replacement part be replaced on Nov. 12, 2009, between 8:00 AM and 6:00 PM. Accordingly, a time stamp date of Nov. 12, 2009 and a
20 time stamp time of 16:33:42:05 may provide validation that the replacement part was replaced within the specified date and time interval.

An encryption operation 652 may then be performed on new source unique system identifier 650 to generate a new
25 encrypted unique system identifier 628. As an example, the encryption operation may be performed using a private key associated with the target system and a public key associated with the provider of the replacement system component. The new encrypted unique system identifier 628
30 may then be communicated to digital assets entitlement system 218, which may in turn perform a decryption operation 626 to generate a decrypted unique system identifier 622.

As likewise shown in FIGURE 6, ETL and other database operations 634 may be performed on the decrypted unique system identifier 622 to generate new unique system component identifiers 602. As shown in FIGURE 6, the new unique system component identifiers may now comprise Model Number 304 `SA310J43`, Serial Number 306, `SEM5239923875`, Factory ID 308 `AUS`, Timestamp Date 610 `112009`, and Timestamp Time 612 `16:33:42:05`. New unique system component identifiers 602 may likewise comprise New Motherboard ID 314 `56812FR853945PL`, Processor ID 316 `92348430-432919237`, Hard Drive ID 318 `L83747HJ3672`, etc. In some embodiments, Timestamp Date 610 and Timestamp Time 612 may be compared to previously authorized timestamp date and timestamp times to validate the authenticity of new unique system component identifiers 602 and their corresponding decrypted unique system identifier 622. In these and other embodiments, if the decrypted unique system identifier 622 is validated, then a first set of operations may be performed to remove entitlement 330 between the original encrypted unique system identifier and digital assets 332. A second set of operations may then be performed to associate new encrypted unique system identifier 628 with digital assets 332 to generate new entitlement 630. Accordingly, the integrity of the original entitlement between the original encrypted unique system identifier and digital assets 332 may be perpetuated by new entitlement 630 between new encrypted unique system identifier 628 and digital assets 332.

In various other embodiments, the provider of the replacement system component may be able to determine its associated unique system component identifier. In some

embodiments, the unique system component identifier may be known in advance. In other embodiments, the unique system component identifier may be one of a pool of, or a range of, possible unique system component identifiers set aside for replacement purposes. As described in greater detail herein, a new source unique identifier may be generated, using the unique system component identifier of the component to be replaced. Once the new source unique identifier is generated, the unique system component identifier of the replaced system component may be invalidated. In these and other embodiments, the system component may be replaced in the target system, the target system may then be initiated (e.g., booted), and an inventory of unique system component identifiers may be performed. In some embodiments, one or more unique system component identifiers, for example a serial number or service tag, may be visible and may be visually inventoried. In other embodiments, one or more unique system component identifiers, for example a motherboard, processor, or hard drive serial number, may not be visible and may be automatically inventoried.

As shown in FIGURE 6, a new source unique system identifier 650 may be generated from the inventoried unique system component identifiers. In some embodiments, a time stamp date and a time stamp time may be components of new source unique system identifier 650. In these embodiments, the time stamp date and a time stamp time may be used to validate the authenticity of new source unique system identifier 650. An encryption operation 652 may then be performed on new source unique system identifier 650 to generate new encrypted unique system identifier 628. As an example, the encryption operation may be performed using a private key associated with the target system and a public

key associated with the provider of the replacement system component. The new encrypted unique system identifier 628 may then be communicated to a digital assets entitlement system, which in turn may perform a decryption operation 626
5 to generate a decrypted unique system identifier 622.

Comparison operations 654 may then be performed between the new source unique system identifier and decrypted unique system identifier 622. If comparison operations 654 are successful, then a first set of operations may be performed
10 to remove the entitlement 330 between the original encrypted unique system identifier and digital assets 332. A second set of operations may then be performed to associate new encrypted unique system identifier 628 with digital assets 332 to generate a new entitlement 630. Accordingly, the
15 integrity of the original entitlement between the original encrypted unique system identifier and digital assets 332 may be perpetuated by the new entitlement 630 between the new encrypted unique system identifier 628 and the digital assets 332. Skilled practitioners of the art may appreciate
20 that many such embodiments are possible and the foregoing is not intended to limit the spirit, scope, or intent of the disclosure.

FIGURES 7A-B illustrate a flow chart of an example method 700 for performance of digital asset entitlement
25 operations, in accordance with embodiments of the present disclosure. According to certain embodiments, method 700 may begin at step 702. As noted above, teachings of the present disclosure may be implemented in a variety of configurations of system 200. As such, the preferred initialization point
30 for method 700 and the order of the steps 702-734 comprising method 700 may depend on the implementation chosen.

In method 700, digital asset entitlementment operations may be started in step 702, followed by the selection of a target system in step 704 for digital assets entitlementment. The unique system identifier of the target system, as
5 described in greater detail herein, may be determined in step 706, followed by a determination being made in step 708 whether a device record has been established for the target system. If not, then the device record may be generated in step 710. As used herein, a device record may refer to a
10 data record comprising data related to a system which will receive an entitlementment to process associated digital assets. In various embodiments, the unique system identifier of the target system may be stored in the device record. In various embodiments, other records may be associated with the device
15 record to further describe the system, such as, for example, its model, type, make, internal identifiers, etc.

Once the device record has been generated, or if it is determined in step 708 that it has already been established, then a determination may be made in step 712 whether an
20 account record has been established for a user. If not, then the account record may be generated for the user in step 714. As used herein, an account record may refer to a data record comprising data related to the association of multiple devices or systems to one or more entities. In
25 various embodiments, the entity may be a single individual or a group of individuals. As an example, the entity may be a household with multiple PCs, a small business with several employees, a large corporation with many employees, etc. Other records may be attached to the account to further
30 describe the account holder, payment information related to the account, etc. Accounts may further be broken down or organized into sub-accounts as needed (e.g., to describe

departments within an enterprise). In various embodiments, a user may be associated with a single device or system or multiple devices or systems in the account record.

Conversely, a group of users may be associated with a single
5 device or system or multiple devices in the account record.
Further, more groups of individual users may likewise be associated with groups of individual devices or systems. Those of skill in the art may appreciate that many such associations are possible and the foregoing is not intended
10 to limit the spirit, scope, or intent of the disclosure.
Once the account record has been generated, or if it is determined in step 712 that it has already been established, then a determination may be made in step 716 whether the account record may be associated with the target system. If
15 not, then the account record may be associated with the target system in step 718.

Once the account record has been associated with the target system, or if it is determined in step 716 that it has already been associated, then a target list of digital
20 assets may be presented in step 720 for entitlement. A determination may then be made in step 722 whether to generate an entitlement for a digital asset. If not, then a determination may be made in step 732 whether to continue digital asset entitlement operations. If so, then the
25 process may be continued, proceeding with step 704.

Otherwise digital asset entitlement operations may be ended in step 734. However, if it is determined in step 722 to generate an entitlement for a digital asset, then a target digital asset may be selected in step 724. A digital assets
30 entitlement may then be generated in step 726 by performing operations to associate the selected digital asset's corresponding license record with the aforementioned device

record, account record, and/or other predetermined records. The resulting digital assets entitlement association may then be added to the entitlement record in step 728. A determination may then be made in step 730 whether to
5 generate another digital assets entitlement. If so, the process may be continued, proceeding with step 724. Otherwise, a determination may be made in step 732 whether to continue digital asset entitlement operations. If so, then the process may be continued, proceeding with step 704.
10 Otherwise digital asset entitlement operations may be ended in step 734.

Although FIGURES 7A and 7B disclose a particular number of steps to be taken with respect to method 700, method 700 may be executed with greater or lesser steps than those
15 depicted in FIGURES 7A and 7B. In addition, although FIGURES 7A and 7B disclose a certain order of steps to be taken with respect to method 700, the steps comprising method 700 may be completed in any suitable order.

Method 700 may be implemented using information
20 handling system 100, system 200, components thereof, and/or any other system operable to implement method 700. In certain embodiments, method 700 may be implemented partially or fully in software and/or firmware embodied in computer-readable media.

25 FIGURE 8 illustrates a flow chart of an example method 800 for the performance of digital assets migration operations, in accordance with embodiments of the present disclosure. According to certain embodiments, method 800 may begin at step 802. As noted above, teachings of the present
30 disclosure may be implemented in a variety of configurations of system 200. As such, the preferred initialization point

for method 800 and the order of the steps 802-830 comprising method 800 may depend on the implementation chosen.

In method 800, digital assets migration operations may begin in step 802. A determination may be made in step 804
5 whether a personalization agent is loaded on the source system. If it is determined in step 804 that a personalization agent is not loaded on the source system, then it may be loaded in step 806. In either case, the personalization agent may query the target system to
10 determine its unique system identifier in step 808. After the system identifier is determined in step 808, inventory operations may then be performed in step 810 by the personalization agent to inventory digital assets and any associated digital assets entitlement data installed on the
15 source system.

The personalization agent may then automatically establish a communicative session with the digital assets entitlement system in step 812 and use the unique system identifier to authenticate the source system and upload the
20 inventoried digital assets and digital assets entitlement data associated with the source system. The digital assets entitlement system may then perform comparison operations in step 814 between the digital assets and the digital assets entitlement data respectively corresponding to the source
25 system's and the target system's unique system identifiers. A determination may then be made in step 816 if all of the inventoried digital assets and digital assets entitlement data associated with the source system's unique system identifier is now associated with the target system's unique
30 system identifier.

If not, then the digital assets and digital assets entitlement data not associated with the unique system

identifier of the target system may be determined in step 818. The user may then be prompted in step 820 to provide any missing license keys, or other digital assets entitlement data, associated with inventoried digital assets that are not currently associated with the target system's unique system identifier. The user may then provide the requested digital assets license keys or other missing digital assets entitlement data to the digital assets entitlement system in step 822.

Digital assets entitlement data may then be generated in step 824 by binding the digital assets and their associated activated activation key or other digital assets entitlement data to the unique system identifier of the source system. The bound data may then be stored in the digital assets entitlement system in step 826. The entitlement of the digital assets is then migrated in step 828 by disassociating their respective digital assets entitlements from the unique system identifier of the source system and then associating it with the unique system identifier of the target system. Then, or if it is determined in step 816 that all inventoried digital assets data and associated digital assets entitlement data is currently on the digital assets entitlement system, digital assets migration operations may end in step 830.

Although FIGURE 8 discloses a particular number of steps to be taken with respect to method 800, method 800 may be executed with greater or lesser steps than those depicted in FIGURE 8. For example, in some embodiments, step 828 of method 800, in which digital assets are disassociated with a source system during migration, may be omitted. Such omission may occur in situations in which license terms allow a digital asset to remain authorized for use on a

source system after migration to a target system is complete. In addition, although FIGURE 8 discloses a certain order of steps to be taken with respect to method 800, the steps comprising method 800 may be completed in any
5 suitable order.

Method 800 may be implemented using information handling system 100, system 200, components thereof, and/or any other system operable to implement method 800. In certain embodiments, method 800 may be implemented partially
10 or fully in software and/or firmware embodied in computer-readable media.

FIGURE 9 illustrates a flow chart of an example method 900 for migrating digital assets between a target system and a cloud storage provider, in accordance with embodiments of
15 the present disclosure. In some embodiments, one or more portions of method 900 may execute contemporaneously with one or more portions of method 800 described above. According to certain embodiments, method 900 may begin at step 902. As noted above, teachings of the present
20 disclosure may be implemented in a variety of configurations of system 200. As such, the preferred initialization point for method 900 and the order of the steps 902-918 comprising method 900 may depend on the implementation chosen.

In method 900, digital assets migration operations may
25 begin in step 902. At step 904, a personalization agent, a digital assets entitlement system, or another component may initiate migration of digital assets to a target system from a data protection store having stored therein backup data associated with a source system. In some embodiments, such
30 migration may occur in a "last in, first-out" order, such that snapshots of source system data stored on the data

protection store are migrated to the target system in reverse chronological order of the snapshots.

At step 906, while data is being migrated from the data protection store to the target system, a data protection agent of the source system may continue generating snapshots at regular intervals. At step 908, the data protection agent may communicate the snapshot to the data protection store.

At step 910, the data protection store may, as it receives additional snapshots from the source system during the migration process, migrate such snapshots to the target system.

At step 912, the data protection store, the digital assets entitlement system, the target system, or another component may determine if all information in the data protection store has been migrated to the target system. If all of the data protection store data has been migrated, method 900 may proceed to step 914. Otherwise, if not all of the data protection store data has been migrated, method 900 may proceed again to step 906.

At step 914, the data protection agent or another component may determine if any changes to the source system data have been made since the last snapshot. If no changes have been made, method 900 may proceed to 916. Otherwise, if changes have been made, method 900 may proceed again to step 906.

At step 916, the data protection agent, personalization agent, digital assets entitlement system, target system, and/or another component may communicate an alert to the user that the migration has completed.

At step 918, method 900 may end.

Although FIGURE 9 discloses a particular number of steps to be taken with respect to method 900, method 900 may be executed with greater or lesser steps than those depicted in FIGURE 9. In addition, although FIGURE 9 discloses a
5 certain order of steps to be taken with respect to method 900, the steps comprising method 900 may be completed in any suitable order.

Method 900 may be implemented using information handling system 100, system 200, components thereof, and/or
10 any other system operable to implement method 900. In certain embodiments, method 900 may be implemented partially or fully in software and/or firmware embodied in computer-readable media.

Using the method and systems described herein, a
15 migration would not require a massive transfer of data from a source system at the time of migration, as is the case in traditional migration approaches. Instead, data already present on a data protection store may be supplemented with additional snapshots from a source system, and such data may
20 be migrated to a target system, potentially reducing the data transfer time of data from the source system. In addition, any user downtime associated with migration may be reduced or eliminated. Because the migration may begin with source system data already stored to the data protection
25 store, significant data may be transferred to the target system without burdening the resources of the source system during migration, thus allowing the user to continue using the source system during migration. Any changes to data on the source system during migration may be communicated to
30 the data protection store, which in turn may supplement the data being migrated to the target system. Thus, the user may continue to use the source system until migration is

complete, at which time the user can begin using the fully-migrated target system.

The present disclosure is well adapted to attain the advantages mentioned as well as others inherent therein.

5 While the present disclosure has been depicted, described, and is defined by reference to particular embodiments of the disclosure, such references do not imply a limitation on the disclosure, and no such limitation is to be inferred. The disclosure is capable of considerable modification,
10 alteration, and equivalents in form and function, as will occur to those ordinarily skilled in the pertinent arts. The depicted and described embodiments are examples only, and are not exhaustive of the scope of the disclosure.

For example, the above-discussed embodiments include
15 software modules that perform certain tasks. The software modules discussed herein may include script, batch, or other executable files. The software modules may be stored on a machine-readable or computer-readable storage medium such as, for example, a disk drive. Storage devices used for
20 storing software modules in accordance with embodiments of the disclosure may be magnetic floppy disks, hard disks, or optical discs such as CD-ROMs or CD-Rs, for example. A storage device used for storing firmware or hardware modules in accordance with embodiments of the disclosure may also
25 include a semiconductor-based memory, which may be permanently, removably or remotely coupled to a microprocessor/memory system. Thus, the modules may be stored within a computer system memory to configure the computer system to perform the functions of the module.
30 Other new and various types of computer-readable storage media may be used to store the modules discussed herein. Additionally, those skilled in the art will recognize that

the separation of functionality into modules is for illustrative purposes. Alternative embodiments may merge the functionality of multiple modules into a single module or may impose an alternate decomposition of functionality of modules. For example, a software module for calling sub-modules may be decomposed so that each sub-module performs its function and passes control directly to another sub-module.

Accordingly, although the present disclosure has been described in detail, it should be understood that various changes, substitutions, and alterations can be made hereto without departing from the spirit and the scope of the disclosure as defined by the appended claims.

WHAT IS CLAIMED IS:

1. An information handling system for migrating digital assets, comprising:

5 a storage medium configured to store data comprising backup data associated with a source system; and

a processor configured to:

migrate the data from the storage medium to a target system;

10 during migration of the data from the storage medium to the target system, receive additional data comprising additional backup data associated with the source system and store the additional data to the storage medium; and

15 migrate the additional data to the target system.

2. The information handling system of Claim 1, the data and additional data comprising a plurality of chronological snapshots of data, each snapshot comprising a change in data of the source system occurring since the
20 chronologically preceding snapshot.

3. The information handling system of Claim 2, wherein snapshots making up the data and the additional data are migrated to the target system in reverse chronological
25 order of the snapshots.

4. The information handling system of Claim 1, the processor further configured to:

determine if all data and additional data has been migrated to the target system;

5 determine if any changes have been made to the source system since the last receipt of additional data from the source system; and

responsive to determining that all data and additional data has been migrated to the target system and no changes
10 have been made to the source system since the last receipt of additional data from the source system, communicate an alert to a user that migration has completed.

5. A computer-implemented method for migrating digital assets, comprising:

migrating, from a storage medium configured to store data comprising backup data associated with a source system, the data to a target system;

while migrating the data from the storage medium to the target system, receiving additional data comprising additional backup data associated with the source system and storing the additional data to the storage medium; and
migrating the additional data to the target system from the storage medium.

6. The method of Claim 5, the data and additional data comprising a plurality of chronological snapshots of data, each snapshot comprising a change in data of the source system occurring since the chronologically preceding snapshot.

7. The method of Claim 6, wherein snapshots making up the data and the additional data are migrated to the target system in reverse chronological order of the snapshots.

8. The method of Claim 5, further comprising:
determining if all data and additional data has been
migrated to the target system;
determining if any changes have been made to the source
5 system since the last receipt of additional data from the
source system; and
responsive to determining that all data and additional
data has been migrated to the target system and no changes
have been made to the source system since the last receipt
10 of additional data from the source system, communicating an
alert to a user that migration has completed.

9. An article of manufacture comprising:
a computer readable medium; and
computer-executable instructions carried on the
computer readable medium, the instructions readable by a
processor, the instructions, when read and executed, for
5 causing the processor to:
migrate, from a storage medium configured to store
data comprising backup data associated with a source
system, the data to a target system;
10 while migrating the data from the storage medium
to the target system, receive additional data
comprising additional backup data associated with the
source system and store the additional data to the
storage medium; and
15 migrate the additional data to the target system
from the storage medium.

10. The article of Claim 9, the data and additional
data comprising a plurality of chronological snapshots of
20 data, each snapshot comprising a change in data of the
source system occurring since the chronologically preceding
snapshot.

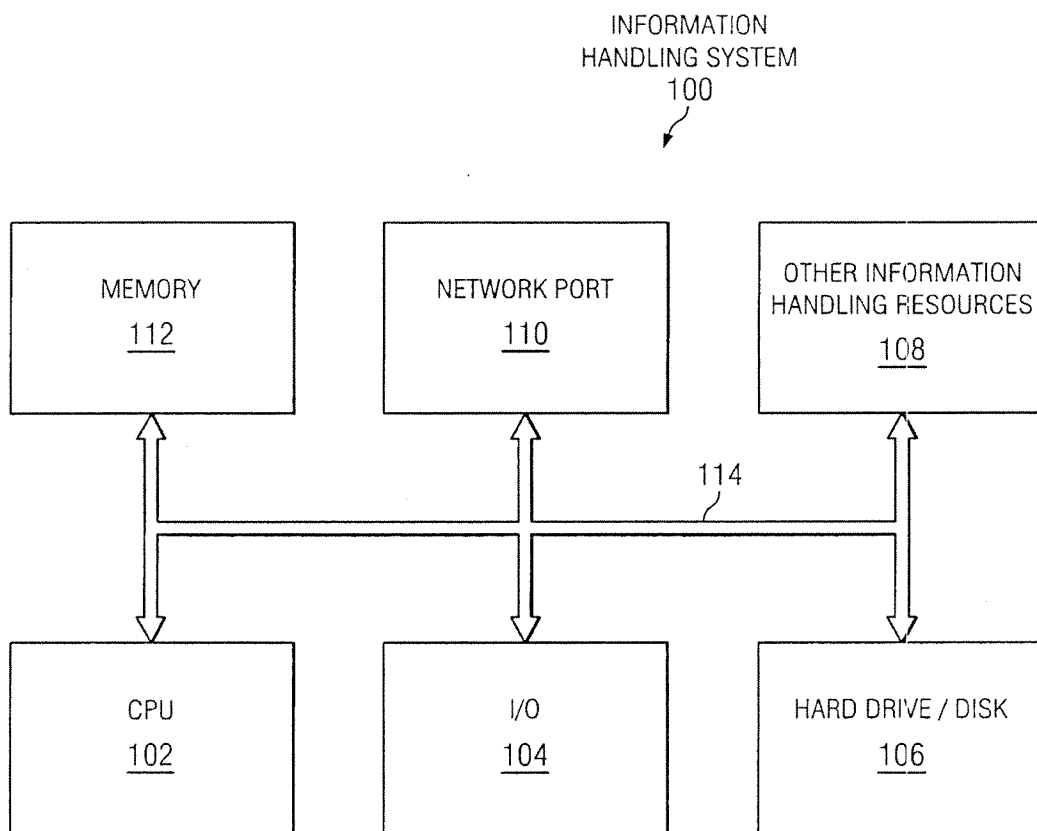
11. The article of Claim 10, wherein snapshots making
25 up the data and the additional data are migrated to the
target system in reverse chronological order of the
snapshots.

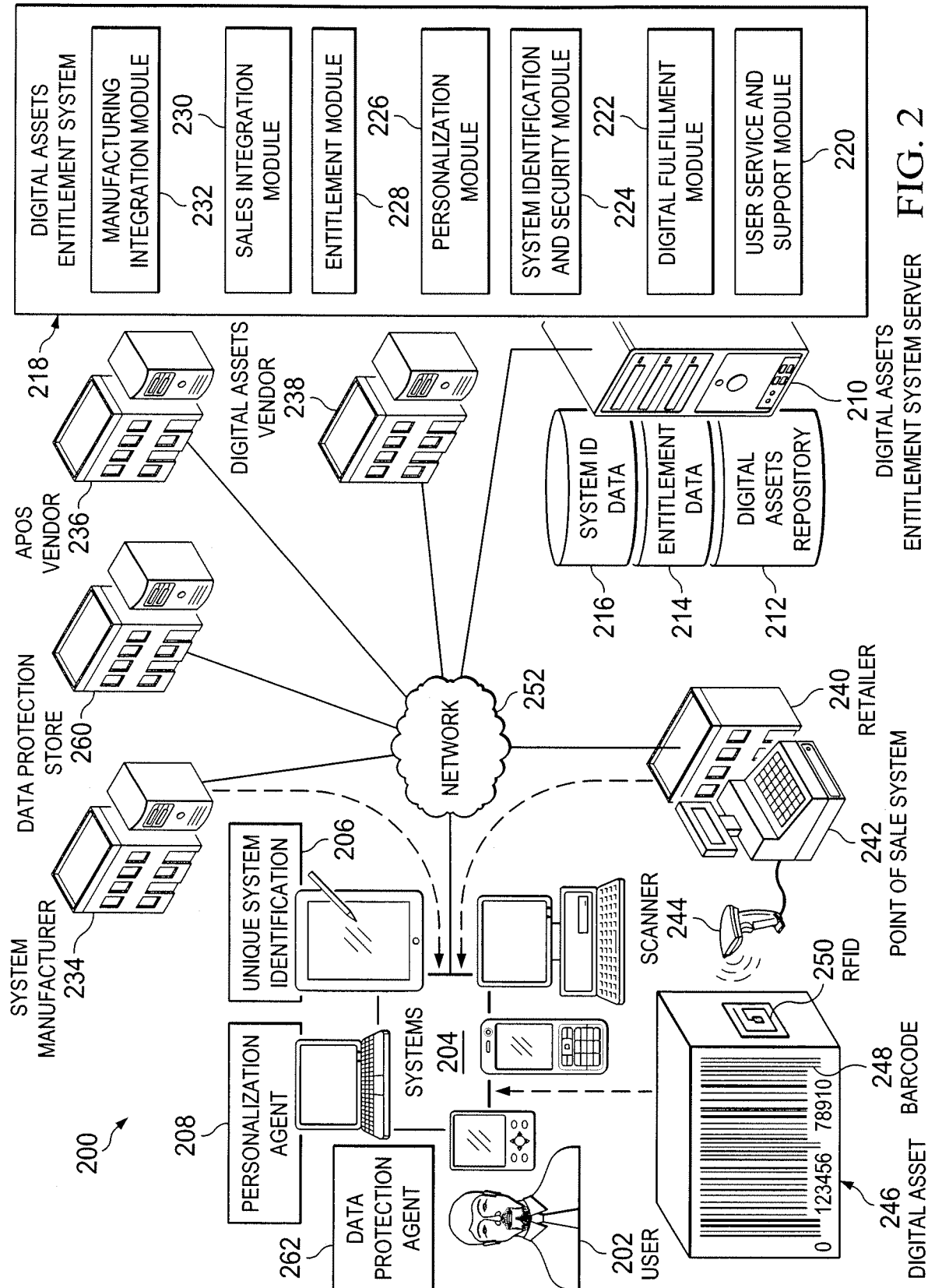
12. The article of Claim 9, the processor for further causing the processor to:

determine if all data and additional data has been migrated to the target system;

5 determine if any changes have been made to the source system since the last receipt of additional data from the source system; and

responsive to determining that all data and additional data has been migrated to the target system and no changes
10 have been made to the source system since the last receipt of additional data from the source system, communicate an alert to a user that migration has completed.

*FIG. 1*



DIGITAL ASSETS ENTITLEMENT SYSTEM SERVER FIG. 2

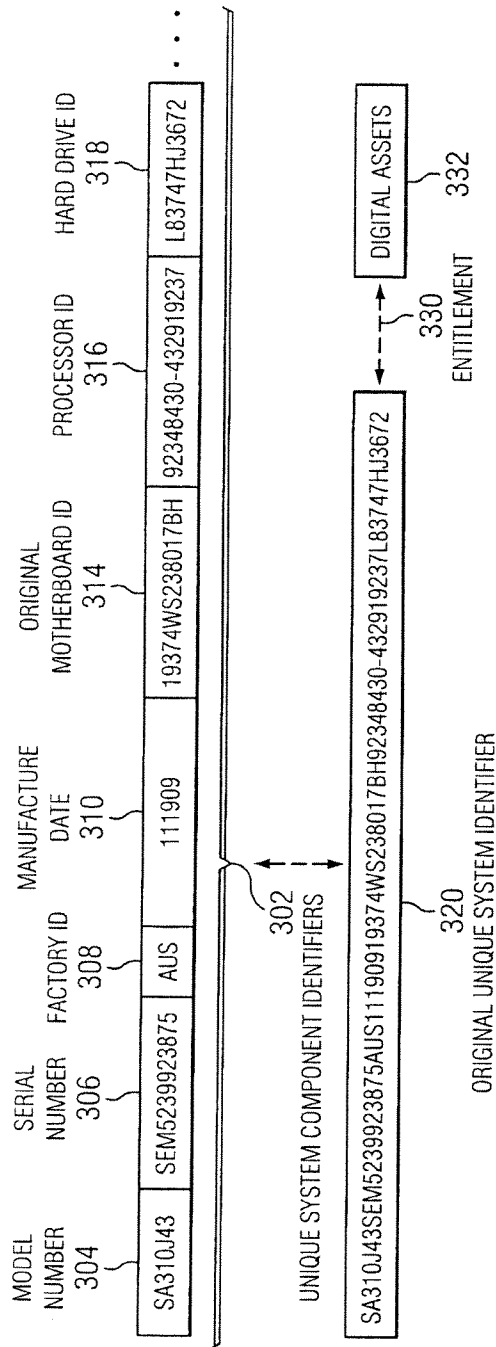


FIG. 3A

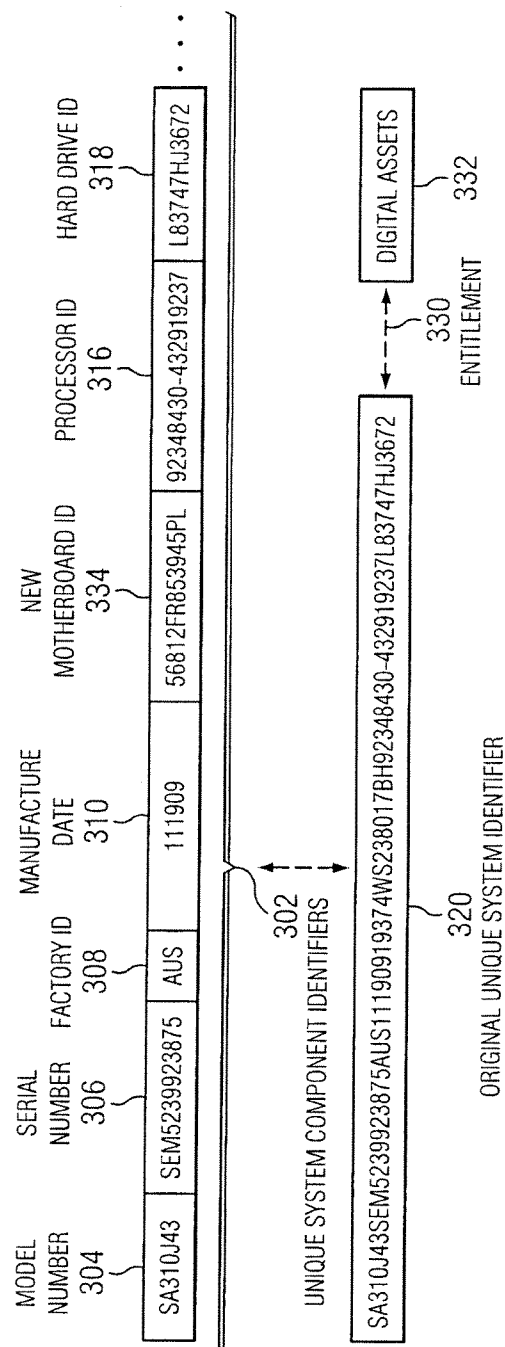


FIG. 3B

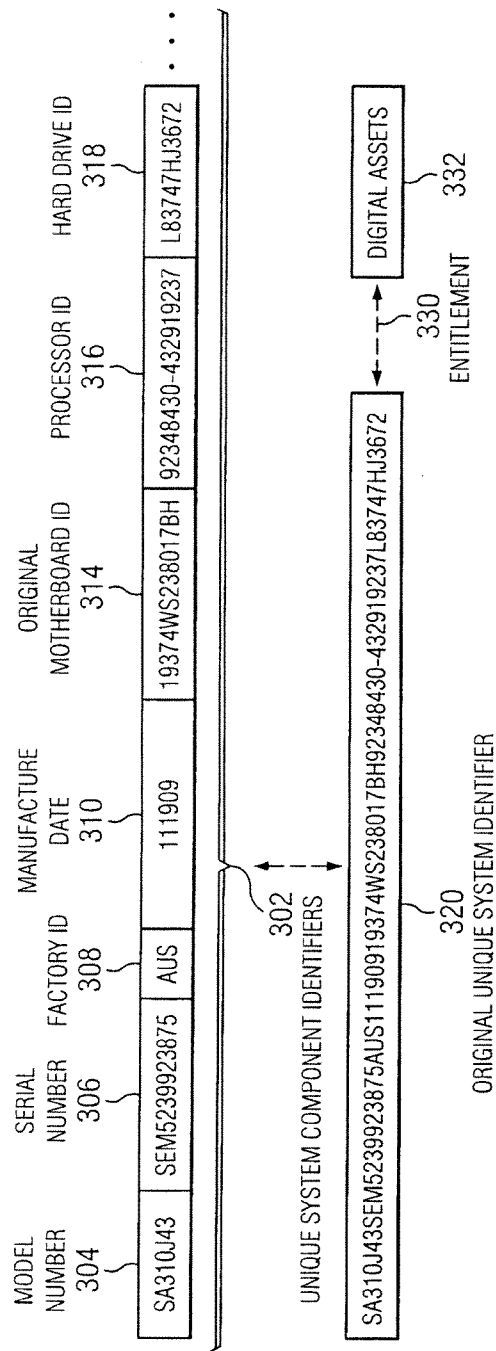


FIG. 4A

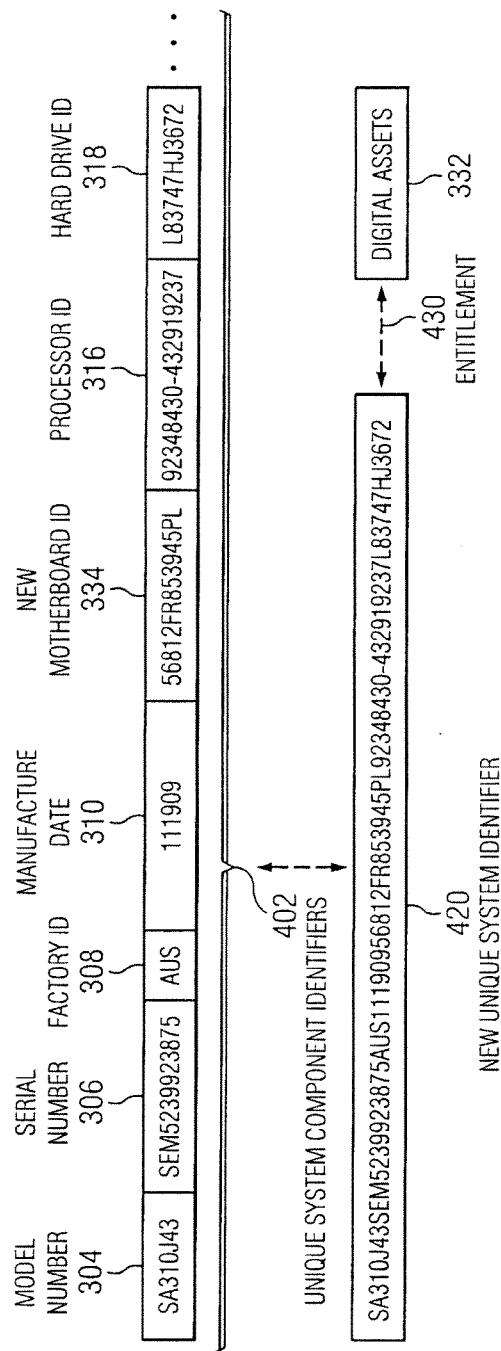


FIG. 4B

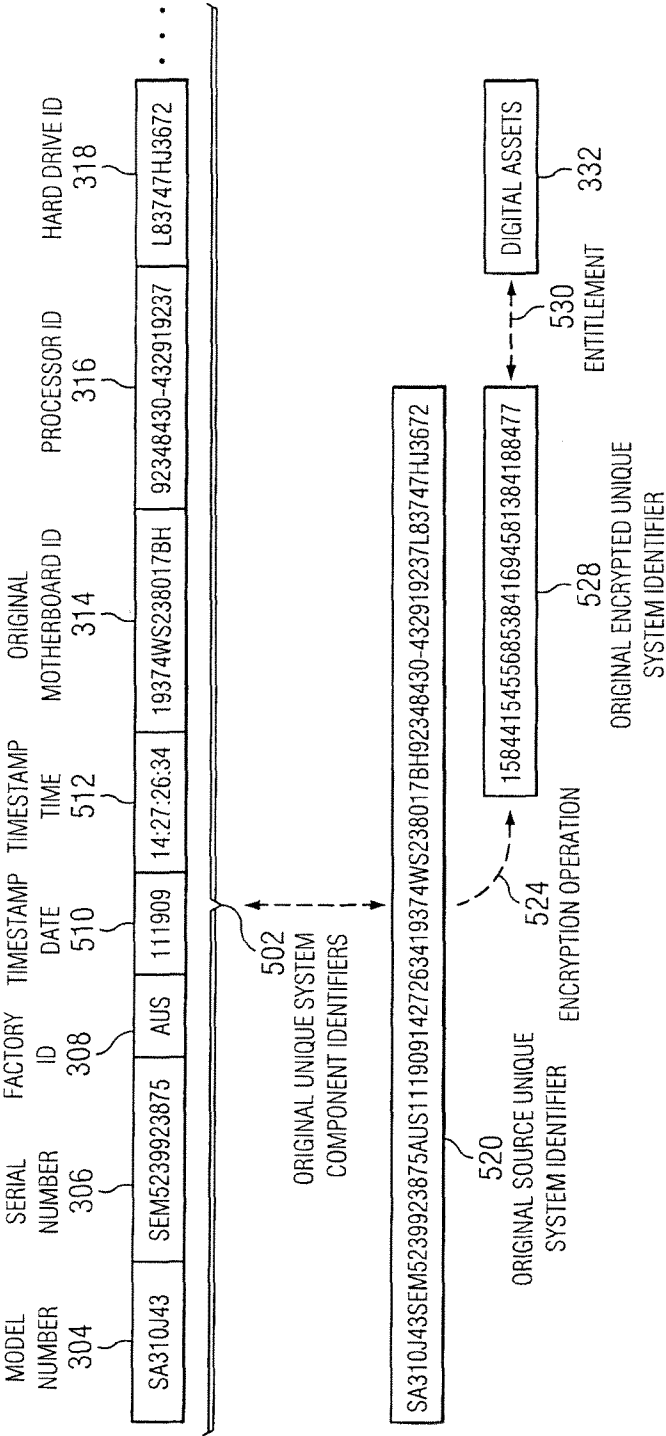


FIG. 5

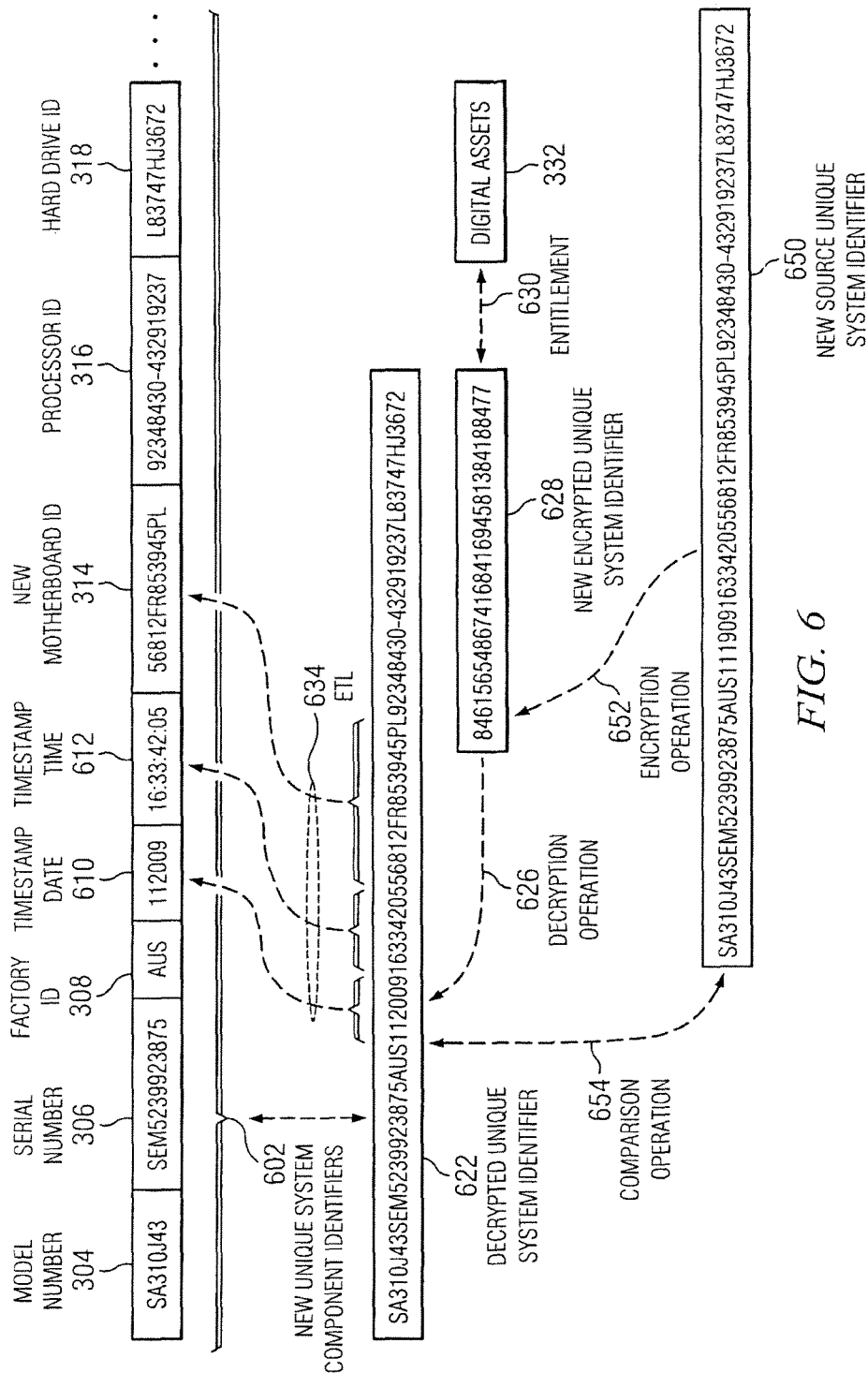
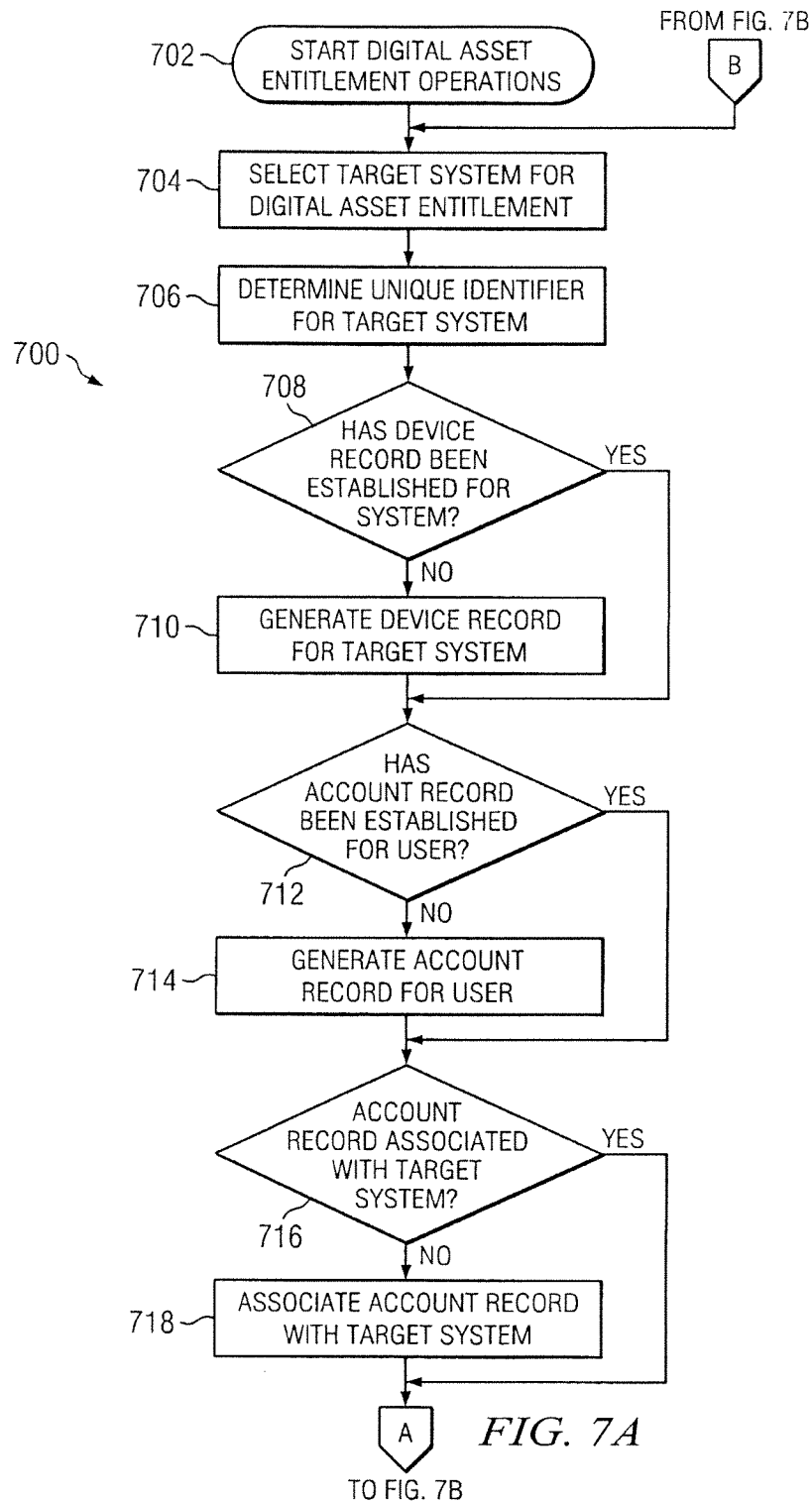


FIG. 6



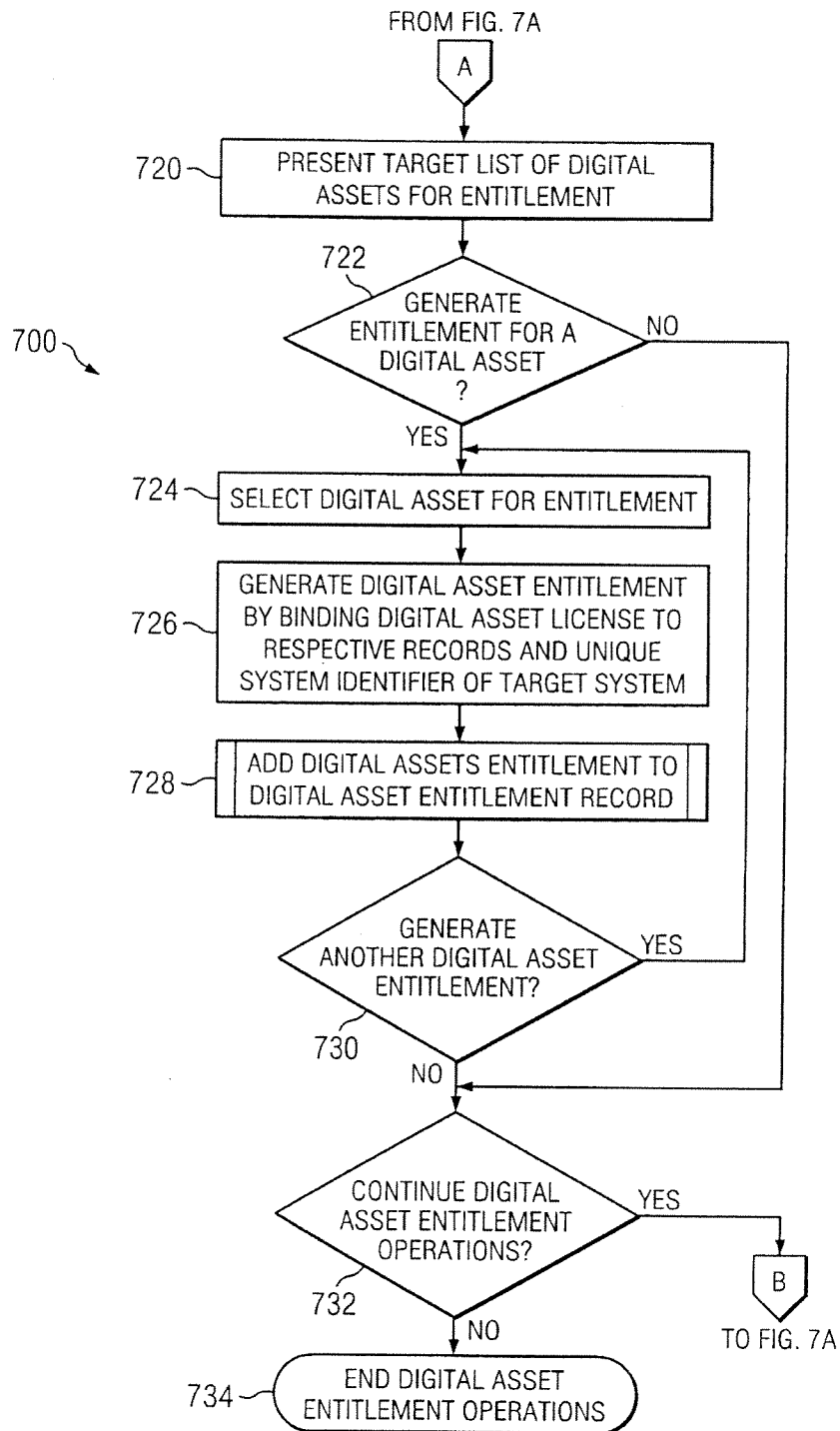
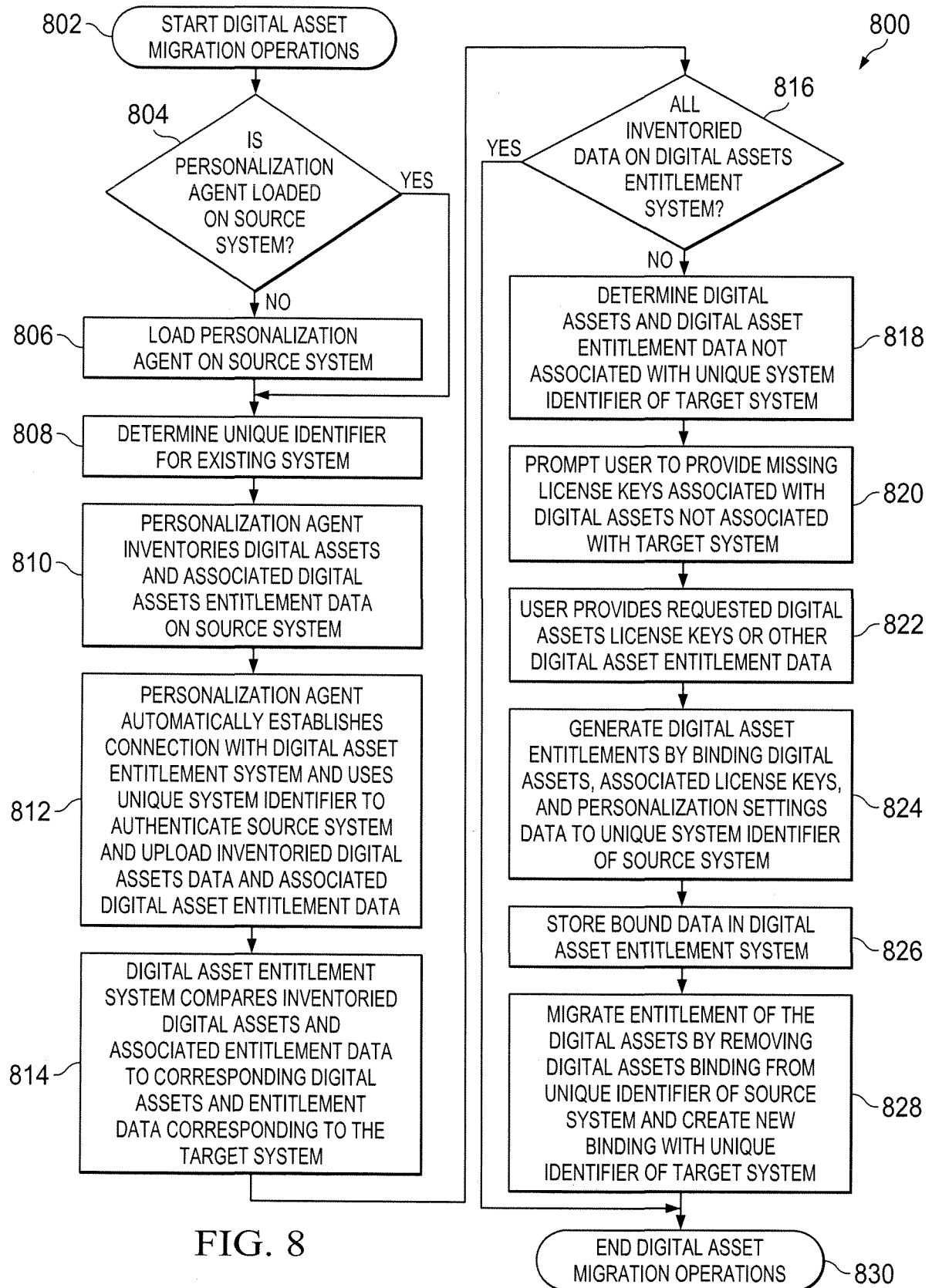


FIG. 7B



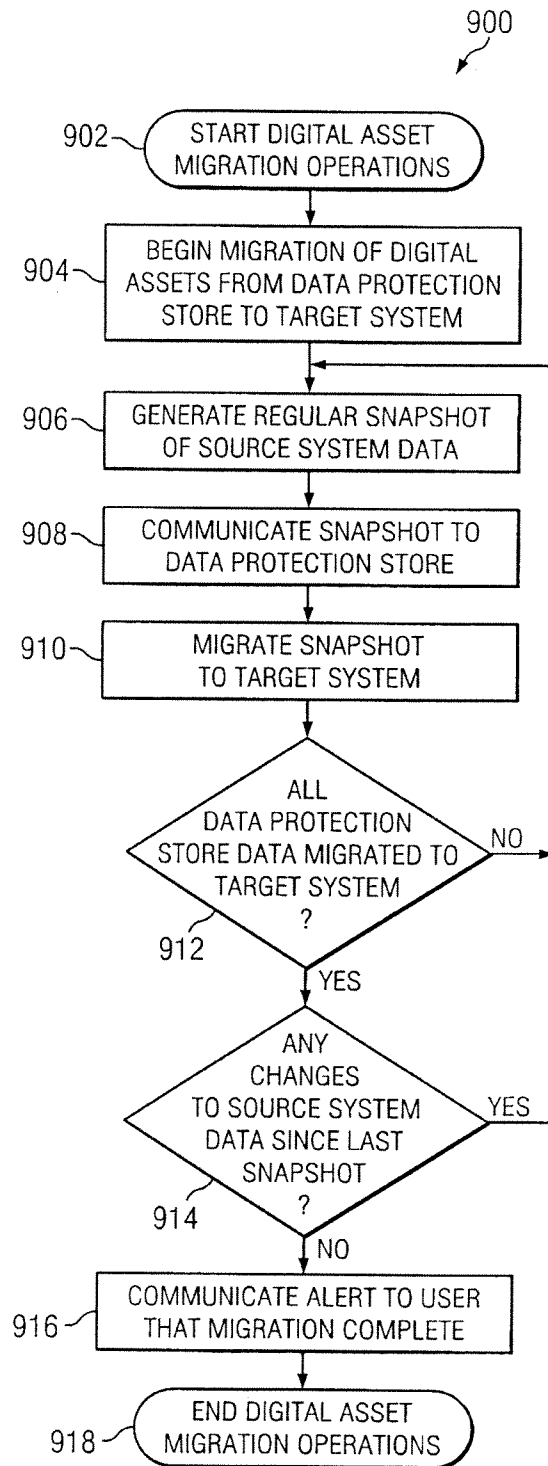


FIG. 9

A. CLASSIFICATION OF SUBJECT MATTER**G06F 12/16(2006.01)i, G06F 13/14(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 12/16; G06F 17/30; G06F 12/00; G06F 13/14

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords:backup, snapshot, additional, change, update, data, and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012-0209812 A1 (ANGSHUMAN BEZBARUAH et al.) 16 August 2012 See paragraphs [0002]-[0004], [0011]-[0012], [0017]-[0026], [0031]-[0041], and [0045]-[0062]; and figures 1-4.	1-3,5-7,9-11
Y		4,8,12
Y	US 2009-0282203 A1 (NILS HAUSTEIN et al.) 12 November 2009 See paragraphs [0004] and [0019]-[0033]; and figure 4.	4,8,12
A		1-3,5-7,9-11
A	US 2008-0177961 A1 (JEFFREY A. MCSHARRY et al.) 24 July 2008 See paragraphs [0022]-[0025]; and figure 2.	1-12
A	US 2012-0124306 A1 (PHILIP J. ABERCROMBIE et al.) 17 May 2012 See paragraphs [0036], [0090]-[0096], and [0129]-[0141]; and figure 1.	1-12
A	US 2008-0307018 A1 (ROBERT ULRICH et al.) 11 December 2008 See paragraphs [0031]-[0038] and [0045]-[0051]; and figure 3.	1-12
A	US 2007-0079089 A1 (RICHARD S. OHRAN et al.) 05 April 2007 See paragraphs [0012]-[0016], [0040]-[0046], and [0053]-[0066]; and figures 2-4 and 8B.	1-12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

09 August 2013 (09.08.2013)

Date of mailing of the international search report

12 August 2013 (12.08.2013)

Name and mailing address of the ISA/KR

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

Facsimile No. +82-42-472-7140

Authorized officer

NHO Ji Myong

Telephone No. +82-42-481-8528



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/040355

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0209812 A1	16/08/2012	CN 102646064 A	22/08/2012
US 2009-0282203 A1	12/11/2009	US 8090917 B2	03/01/2012
US 2008-0177961 A1	24/07/2008	None	
US 2012-0124306 A1	17/05/2012	CA 2817592 A1	24/05/2012
		US 2012-0123999 A1	17/05/2012
		US 2012-0124012 A1	17/05/2012
		US 2012-0124013 A1	17/05/2012
		US 2012-0124014 A1	17/05/2012
		US 2012-0124046 A1	17/05/2012
		US 2012-0124105 A1	17/05/2012
		US 2012-0124307 A1	17/05/2012
		US 8299944 B2	30/10/2012
		US 8396905 B2	12/03/2013
		US 8402004 B2	19/03/2013
		US 8417674 B2	09/04/2013
		WO 2012-067964 A1	24/05/2012
US 2008-0307018 A1	11/12/2008	US 8468136 B2	18/06/2013
US 2007-0079089 A1	05/04/2007	AU 2002-350221 A1	17/06/2003
		CN 1596400 A	16/03/2005
		CN 1596400 C	20/12/2006
		EP 1449088 A1	25/08/2004
		EP 1449088 A4	26/12/2007
		JP 2005-512191 A	28/04/2005
		JP 4181044 B2	12/11/2008
		KR 10-0560726 B1	14/03/2006
		US 2003-0101321 A1	29/05/2003
		US 7296125 B2	13/11/2007
		US 7398366 B2	08/07/2008
		WO 03-048941 A1	12/06/2003