



(51) International Patent Classification:

G06Q 10/00 (2012.01) *G06Q 50/26* (2012.01)

(21) International Application Number:

PCT/PL2016/050022

(22) International Filing Date:

20 May 2016 (20.05.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **MOTOROLA SOLUTIONS, INC.** [US/US];
1303 East Algonquin Road, Schaumburg, Illinois 60196
(US).(72) Inventors: **FLOWERDAY, David B.**; 560 Golfview Drive,
North Barrington, Illinois 60010 (US). **ORLOWSKI, Remigiusz**;
Brzaczowice 190, 32-410 Dobczyce (PL). **TINE, Steven D.**;
580 Jarvis St, Cheshire, Connecticut 06410 (US). **RADWANSKI, Lechoslaw**;
ul. Szpitalna 28/3, 32-600 Oswiecim (PL).(74) Agent: **TAGOWSKA, Magdalena**; Patpol, ul.
Nowoursynowska 162J, 02-776 Warszawa (PL).(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA,
LC, LK, LR, LS, 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, SA, 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, ST, 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,
KM, ML, MR, NE, SN, TD, TG).

Published:

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

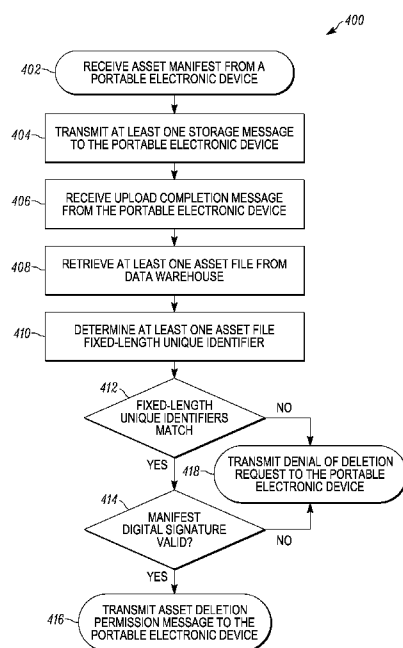
(54) Title: SYSTEMS AND METHODS FOR MAINTAINING CHAIN OF CUSTODY FOR ASSETS OFFLOADED FROM A
PORTABLE ELECTRONIC DEVICE

FIG. 4

(57) Abstract: Systems and methods for maintaining chain of custody for assets offloaded from a portable electronic device. One exemplary system includes an electronic processor configured to receive, from the portable electronic device, an asset manifest including an asset identifier, a fixed-length unique identifier associated with the asset identifier, and a manifest digital signature. The electronic processor is further configured to transmit to the portable electronic device a storage message based on the asset manifest; receive, from the portable electronic device, an upload completion message; retrieve, from a data warehouse an asset file; and determine, for the asset file, an asset file fixed-length unique identifier. The electronic processor is further configured to determine whether the fixed-length unique identifier matches the asset file fixed-length unique identifier; determine whether the manifest digital signature is valid; and to transmit an asset deletion permission message when identifiers match and the digital signature is valid.



SYSTEMS AND METHODS FOR MAINTAINING CHAIN OF CUSTODY FOR ASSETS
OFFLOADED FROM A PORTABLE ELECTRONIC DEVICE

BACKGROUND OF THE INVENTION

[0001] Portable electronic devices (for example, body-worn cameras) are used by law enforcement and other personnel to capture multimedia assets (for example, video recordings, audio recordings, digital photographs, and the like). Metadata relating to the multimedia assets may also be created and stored on the portable electronic devices. Some multimedia assets, and their associated metadata, may need to be preserved (for example, to comply with public records laws). Some multimedia assets and metadata may be used as evidence in criminal trials or other official investigations or proceedings. When used in such proceedings, demonstrating the authenticity of multimedia assets may be mandated by applicable law.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0002] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed invention, and explain various principles and advantages of those embodiments.

[0003] FIG. 1 is a diagram of an asset management system in accordance with some embodiments.

[0004] FIG. 2 is a diagram of an asset management controller in accordance with some embodiments.

[0005] FIG. 3 is a flowchart of a method for offloading assets from a portable electronic device, in accordance with some embodiments.

[0006] FIG. 4 is a flowchart of a method of maintaining chain of custody for assets offloaded from the portable electronic device, in accordance with some embodiments.

[0007] FIG. 5 is a flowchart of sub-method of maintaining chain of custody for assets offloaded from the portable electronic device, in accordance with some embodiments.

[0008] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention.

[0009] The apparatus and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

DETAILED DESCRIPTION OF THE INVENTION

[0010] One exemplary embodiment provides a system for maintaining chain of custody for assets offloaded from a portable electronic device. The system includes an asset management controller, which includes a network interface and an electronic processor coupled to the network interface. The electronic processor is configured to receive, from the portable electronic device via the network interface, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier associated with the at least one asset identifier, and a manifest digital signature. The electronic processor is further configured to transmit, to the portable electronic device via the network interface, at least one storage message based on the asset manifest. The electronic processor is further configured to receive, from the portable electronic device via the network interface, an upload completion message. The electronic processor is further configured to retrieve, from a data warehouse via the network interface, at least one asset file. The electronic processor is further configured to determine, for the at least one asset file, at least one asset file fixed-length unique identifier. The electronic processor is further configured to determine whether the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier. The electronic processor is further configured to determine whether the manifest digital signature is valid. The electronic processor is further configured to transmit, via the network interface, an asset deletion permission

message when the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, and the manifest digital signature is valid.

[0011] Another exemplary embodiment provides a method for maintaining chain of custody for assets offloaded from a portable electronic device. The method includes receiving, by an electronic processor, via a network interface coupled to the electronic processor, from the portable electronic device, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier associated with the at least one asset identifier, and a manifest digital signature. The method further includes transmitting, by the electronic processor via the network interface, to the portable electronic device, at least one storage message based on the asset manifest. The method further includes receiving, by the electronic processor via the network interface, from the portable electronic device, an upload completion message. The method further includes retrieving, by the electronic processor via the network interface, at least one asset file from a data warehouse. The method further includes determining, by the electronic processor, for the at least one asset file, at least one asset file fixed-length unique identifier. The method further includes determining, by the electronic processor, whether the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier. The method further includes determining, by the electronic processor, whether the manifest digital signature is valid. The method further includes transmitting, by the electronic processor via the network interface, an asset deletion permission message when the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, and the manifest digital signature is valid.

[0012] For ease of description, each of the exemplary systems presented herein is illustrated with a single exemplar of each of its component parts. Some examples may not describe or illustrate all components of the systems. Other exemplary embodiments may include more or fewer of each of the illustrated components, may combine some components, or may include additional or alternative components.

[0013] FIG. 1 is a diagram of one exemplary embodiment of an asset management system 10. The terms “asset,” “asset file,” and “multimedia asset,” as used herein, refer to multimedia files (for example, video recordings, audio recordings, digital

photographs, and the like) captured and stored by operation of the asset management system 10. The asset management system 10 includes a network 12, a portable electronic device 14, an asset management controller 16, an asset management database 18, a first data warehouse 20, and a second data warehouse 22. The exemplary asset management system 10 illustrated in FIG. 1 is a public safety asset management system—though other embodiments of the asset management system 10 are not limited to public safety applications.

[0014] In one example, the portable electronic device 14 may be used by a law enforcement agency to capture and store a multimedia asset (for example, a video) of a robbery 24. The portable electronic device 14 may also receive and store metadata relating to the asset. As described in greater detail below, embodiments of the asset management system 10 are configured to offload the captured asset and its associated metadata from the portable electronic device 14, and place the asset in long-term storage (for example, the first data warehouse 20 or the second data warehouse 22). The asset may then be used as evidence in criminal justice proceedings related to the robbery 24, or in other ways.

[0015] The network 12 may be a wired or wireless network. All or parts of the network 12 may be implemented using various existing networks, for example, a cellular network, the Internet, a land mobile radio (LMR) network, a Bluetooth™ network, a wireless local area network (for example, Wi-Fi), a wireless accessory Personal Area Networks (PAN), a Machine-to-machine (M2M) autonomous network, and a public switched telephone network. The network 12 may also include future developed networks. The portable electronic device 14, the asset management controller 16, the asset management database 18, the first data warehouse 20, and the second data warehouse 22 communicate with each other over the network 12 using suitable wireless or wired communications protocols. In some embodiments, communications with other external devices (not shown) occurs over the network 12.

[0016] In the example illustrated, the portable electronic device 14 is a body-worn camera, for example, one of the Motorola® Si series of video speaker microphones. The portable electronic device 14 includes components (for example, a digital camera, a microphone, a microprocessor, memory, and a network interface) for capturing,

storing, and transmitting multimedia assets (for example, over the network 12). Embodiments of the portable electronic device 14 also include hardware and software (for example, buttons, a touchscreen, and a user interface) for receiving user inputs and other data. Other components (not shown) may be included to provide different functions (for example, radio communications). In alternative embodiments, the portable electronic device 14 may be a handheld communication device (for example, a mobile telephone, portable two-way radio, or other portable communication device), a smart watch or other smart wearable, or other electronic device capable of capturing assets and communicating over the network 12.

[0017] The asset management controller 16, described in greater detail below, communicates with, and controls the portable electronic device 14 to offload and store assets (for example, in the first data warehouse 20 and the second data warehouse 22). The asset management controller 16 is communicatively coupled to the asset management database 18, which electronically stores information regarding the offloaded assets in a relational database. The asset management controller 16 reads and writes such information to and from the asset management database 18, which database may be housed on a suitable database server (not shown); integrated with, or internal to, the asset management controller 16; or external to the asset management system 10 and accessible over the network 12.

[0018] The first data warehouse 20 is a central repository for storing data electronically. The first data warehouse 20 is capable of communicating and exchanging data with the portable electronic device 14 and the asset management controller 16 over the network 12. In some embodiments, the first data warehouse 20 is a commercial cloud-based storage service such as, for example, the Amazon™ Simple Storage Service (Amazon S3). In some embodiments, the first data warehouse 20 is a data storage system provided internally by the agency that owns and operates the asset management system 10. The first data warehouse 20 may be compliant with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) standard. The second data warehouse 22 is similar to the first data warehouse 20 and, collectively, the two examples illustrated are representative of any number of data warehouses, which are capable of communicating and exchanging data with the

portable electronic device 14 and the asset management controller 16 over the network 12. In some embodiments, the asset management system 10 uses a single data warehouse to store offloaded assets; in other embodiments two, three, or more data warehouses may be selected from and used to store offloaded assets.

[0019] FIG. 2 is a diagram of one exemplary embodiment of the asset management controller 16. In the embodiment illustrated, the asset management controller 16 includes an electronic processor 205 (for example, a microprocessor, or other electronic controller), a memory 210, and a network interface 215. The electronic processor 205, the memory 210, and the network interface 215, as well as the other various modules are coupled directly, by one or more control or data buses, or a combination thereof.

[0020] The memory 210 may include read-only memory (ROM), random access memory (RAM), other non-transitory computer-readable media, or a combination thereof. The electronic processor 205 is configured to retrieve instructions and data from the memory 210 and execute, among other things, instructions to perform the methods described herein.

[0021] The electronic processor 205 controls the network interface 215 to send and receive data over the network 12. For example, the network interface 215 may include a transceiver for wirelessly coupling to the network 12. Alternatively, or in addition, the network interface 215 may include a connector or port for receiving a wired connection (for example, Ethernet) to the network 12.

[0022] As noted above, embodiments of the portable electronic device 14 may be body-worn cameras, used by law enforcement personnel to make audio, video, or still picture recordings of incidents (for example, traffic stops, crimes in progress, accident investigations, interactions with members of the public, and the like). The portable electronic device 14 does not have a limited memory capacity, and must therefore occasionally offload the asset files created by recording these incidents to make room for new asset files to be created. An asset may be of an urgent nature (for example, video of an at-large crime suspect) such that it is desirable to provide speedy access to other members of the public safety agency or other agencies. Some assets may need to be preserved (for example, to comply with public records laws). Therefore, there

exists a need to offload the multimedia assets from the portable electronic device by uploading the multimedia assets to an asset management system to facilitate long term storage and retrieval.

[0023] Accordingly, FIG. 3 illustrates an exemplary method 300 for offloading assets from the portable electronic device 14 for long-term storage. At block 302, the electronic processor 205 receives, via the network interface 215 at least one asset upload request from the portable electronic device 14 over the network 12. An asset upload request is a request from the portable electronic device 14 to offload one or more assets stored locally on the portable electronic device 14. Each asset upload request includes an asset manifest and at least one device status indicator.

[0024] An asset manifest includes at least one asset identifier and metadata associated with each of the asset identifiers. In some embodiments, the asset manifest includes at least two asset identifiers. Each asset identifier identifies an asset to be offloaded by the portable electronic device 14. Metadata is data pertaining to an asset, linked to the asset by the asset identifier. Metadata may include a file type (for example, video, audio, or photo), a file size, a timestamp (that is, when the asset was captured), a user role for the user who captured the asset (for example, police officer or supervisor), an incident type (for example, a crime, a traffic stop, and the like), or an incident identifier (for example, from a computer-aided dispatch system). Metadata may also be an asset capture location, such as, for example, the geographic coordinates or an address where the asset was captured, or an indication that the asset was captured within a geographic area (for example, a geofence) that is predefined to be of high interest (for example, a high-crime area or an area surrounding an emergency situation).

[0025] Each device status indicator indicates something about the status of the portable electronic device 14 at the time the asset upload request is made. Device status indicators may include a connected network identifier (that is, which network the device is currently communicating over), nearby network identifiers (for example, nearby Wi-Fi networks to which the portable electronic device 14 may connect), a connected network signal strength (for example, a Wi-Fi signal strength level), a battery level (for example, what percentage of the battery is remaining), a charging

status (for example, receiving a charge), a device location, and a memory usage level (that is, how much storage is still available for capturing and storing assets on the portable electronic device 14).

[0026] For each of the asset identifiers in the asset manifest, the electronic processor 205 determines whether to grant or deny the asset upload request. At block 304, the electronic processor 205 determines whether to grant or deny the asset upload request based on the metadata from the asset manifest and at least one of the device status indicators. For example, when an asset is associated with a high-priority incident, the electronic processor 205 may grant the request. In another example, the connected network identifier may indicate that the portable electronic device 14 is connected to a network which is not suitable for large data transmissions, and the electronic processor 205 may deny the asset upload request. In another example, the battery level may be too low to power the portable electronic device 14 for the duration of the asset upload, and the electronic processor 205 may deny the asset upload request. In another example, the connected network signal strength may be below an acceptable threshold, and the electronic processor 205 may deny the asset upload request. In another example, the charging status may indicate that the device is plugged into a power source, and the electronic processor 205 may grant the request. In another example, the device location may indicate that the device is in an “upload zone” where an upload is more likely to successfully complete (for example, a police administration building), and the electronic processor 205 may grant the request. In another example, the device location may indicate that the device is in a “do not upload zone” where an upload is more likely to start, but then fail (for example, near the edge of a network’s coverage area), and the electronic processor 205 may deny the request. In another example, the memory usage level may indicate that the device must offload its asset(s) soon, and the electronic processor 205 may grant the request.

[0027] When the electronic processor 205 determines to deny the asset identifier, it determines at least one asset upload request retry condition, at block 306.

[0028] For example, if a battery level is too low (for example, 10%), the electronic processor may determine an acceptable battery level (for example, 50%), at which the portable electronic device 14 should retry its asset upload request. In another example,

when the network signal strength is below an acceptable level, the electronic processor may determine acceptable signal strength, at which the portable electronic device 14 should retry its asset upload request. In another example, when the connected network indicator indicates that the portable electronic device is connected to an unsuitable network, and a nearby network indicator indicates that a more suitable network is available, the electronic processor may determine that the portable electronic device 14 should retry its asset upload request when it is connected to the more suitable network. In some embodiments, the electronic processor 205 determines more than one asset upload request retry condition, any one, or some combination of, which must be met before the portable electronic device 14 should retry its asset upload request.

[0029] At block 308, the electronic processor 205 determines whether the asset upload request is complete (that is, whether all asset identifiers have been assigned a grant or a deny). When asset identifiers remain, the electronic processor 205 returns to block 304 and determines whether to grant or deny the next asset identifier in the asset manifest.

[0030] When the electronic processor 205 determines to grant the asset identifier at block 304, it selects a data warehouse for long-term storage of the asset, at block 310. The data warehouse is selected from available data warehouses (for example, the first data warehouse 20 and the second data warehouse 22) based on the asset identifier and the metadata. For example, the file type of the asset may be more suitable to the first data warehouse 20 than the second data warehouse 22. In another example, the first data warehouse 20 may be compliant with the Criminal Justice Information Services standard, while the second data warehouse 22 may not be. In such case, assets related to certain incident types (for example, criminal investigations) may have to be stored on the first data warehouse 20. In another example, assets of a particular type, or relating to particular incidents types, may be stored on a local data warehouse, rather than a cloud-based data warehouse, or vice-versa. In some embodiments, the device status may be used to select the data warehouse. For example, when the connected network is a private network, a privately-hosted data warehouse may be selected. In another example, when the connected network is a public network, a

public data warehouse may be selected. In some embodiments, the cost of a data warehouse is used to select the data warehouse. For example, assets that are low priority, and thus may not be frequently accessed, are suitable for a lower cost “cold storage” data warehouse (for example, the Amazon Glacier™ service).

[0031] At block 312, the electronic processor 205 transmits, via the network interface 215, a storage request to the data warehouse selected at block 310. At block 312, the electronic processor 205 receives, via the network interface 215, a data storage path from the data warehouse. The data storage path is an electronic identifier used to identify where the data should be stored in the data warehouse.

[0032] At block 308, the electronic processor 205 determines whether the asset upload request is complete. As noted above, when asset identifiers remain, the electronic processor 205 returns to block 304. When the electronic processor 205 determines that the asset upload request is complete (that is, all asset identifiers have been assigned a grant or a deny), the electronic processor 205 determines at least one storage message, at block 316. In some embodiments, one storage message is determined for each of the asset identifiers. In other embodiments, a single storage message includes the determinations for each of the asset identifiers. For each asset identifier granted, the storage message identifies the data warehouse and includes the data storage path, which the portable electronic device 14 may use to offload the asset (that is, upload the asset to the data warehouse selected at block 310). For each asset identifier denied, the storage message includes the at least one asset upload request retry condition determined at block 306. Accordingly, a storage message may include grants for all asset identifiers in the asset manifest, denials for all asset identifiers in the asset manifest, or a combination of grants and denials.

[0033] In some embodiments, the electronic processor 205 further determines the storage message based on at least one storage priority (one for each asset) and at least one storage time (one for each asset), each based on the metadata and the asset identifier. For example, it may be desirable to have all assets related to a high-priority incident (for example, an officer-involved shooting) offloaded as soon as possible. All assets, whose metadata includes the incident identifier for the high-priority incident, may be assigned a higher priority for offload than other assets. In such case,

the storage message would include a storage priority indicated that the asset identified by the asset identifier be offloaded before other assets. Similarly, the storage time may be determined based on the metadata for the asset. For example, video assets are larger files than audio assets, and it may be advantageous to offload the video assets during off-peak times when the network 12 is less busy. In one example, the asset upload request received at block 302 may be a request to upload a large video asset of an unimportant event. Such an asset may be allocated a lower priority and assigned an upload time of three A.M.

[0034] In some embodiments, the electronic processor 205 further determines whether the storage message should include data chunking. Data chunking is used to separate (or “chunk”) larger data (for example, a large video file) into discrete similarly-sized parts to make transmission and storage more efficient. When the electronic processor 205 determines data chunking should be used for an asset, the storage request transmitted (at block 312) to the data warehouse includes a chunking request. Similarly, the data storage path received at block 314 is responsive to the data chunking request, and may include more than one storage location, or may indicate a location within the data warehouse particular to chunking. In some embodiments, the data warehouse selected at block 310 is selected based on its ability to accept data chunking requests.

[0035] At block 320, the electronic processor 205 transmits, via the network interface 215, the at least one storage message to the portable electronic device 14. The asset identifiers, the associated metadata, and the storage message are stored by the electronic processor 205 in the asset management database 18. Accordingly, the asset management controller 16 may track the locations of the assets in the data warehouses. Users of the asset management controller 16 may search the metadata to identify assets of interest, and, in turn, retrieve those assets based on the information in the storage message.

[0036] Assets, especially those captured by public safety agencies, may be used for evidence in criminal trials or other official investigations or proceedings, in which the authenticity of the asset is mandated by applicable law. Accordingly, FIG. 4

illustrates an exemplary method 400 for maintaining a chain of custody for assets offloaded from the portable electronic device 14.

[0037] Turning to FIG. 4, at block 402, the electronic processor 205 receives an asset manifest from the portable electronic device 14. This asset manifest is part of an asset upload request, as described above in relation to FIG. 3. Included in the asset manifest, is at least one fixed-length unique identifier (for example, a SHA-256 hash of the asset file). In some embodiments, one fixed-length unique identifier is received for each asset identified in the manifest. The asset manifest further includes an asset manifest digital signature. The asset manifest digital signature is generated by the portable electronic device 14 by signing the manifest with a private key known only to the portable electronic device 14 (for example, using a public-private key encryption algorithm).

[0038] At block 404, the electronic processor 205 transmits, via the network interface 215, at least one storage message to the portable electronic device 14. The storage message is determined based on the asset manifest using the method 300, described above. At block 406, the electronic processor 205, via the network interface 215, receives an upload completion message from the portable electronic device 14, which message indicates that the assets identifiers granted in the storage message have been offloaded (uploaded to the data warehouse(s)). As noted above, the portable electronic device 14 has a limited asset storage capacity. Accordingly, the upload completion message may include a request to delete the assets stored in a local memory of the portable electronic device 14, if those assets have been successfully offloaded (that is, uploaded to a data warehouse using the method 300).

[0039] At block 408, the electronic processor 205 retrieves at least one of the asset files identified in the storage message transmitted at block 404 from the data warehouse identified in the storage message. The electronic processor 205 may temporarily store the retrieved asset file in the memory 210 or the asset management database 18.

[0040] At block 410, the electronic processor 205 determines at least one asset file fixed-length unique identifier (that is, one for each asset file retrieved at block 408). The asset file fixed-length unique identifier is determined similarly to the fixed-length

unique identifier received at block 402. For example, when the fixed-length unique identifier is a SHA-256 hash of the asset file on the portable electronic device 14, then the asset file fixed-length unique identifier is also a SHA-256 hash of the retrieved asset file. When the SHA-256 hash of the asset file created on the portable electronic device 14 matches the SHA-256 hash of the retrieved asset file, the files are identical. Accordingly, at block 412, the electronic processor 205 determines whether the asset file fixed-length unique identifier determined at block 410 matches the fixed-length unique identifier received at block 402.

[0041] When the identifiers match, the electronic processor 205 determines whether the manifest digital signature is valid, at block 414. The electronic processor 205 determines whether the manifest signature is valid using a public key known to both the portable electronic device 14 and the asset management controller 16 using a public key cryptography system (for example, RSA). In some embodiments, the electronic processor 205 may receive from the portable electronic device 14, via the network interface 215, a digital certificate (for example, generated by a certificate authority), which includes the public key. In such embodiments, the electronic processor 205 may validate the digital certificate with the certificate authority prior to using the public key to validate the manifest digital signature. When the manifest signature is valid, the electronic processor 205 transmits, via the network interface 215, an asset deletion permission message to the portable electronic device 14. The asset deletion permission message indicates to the portable electronic device 14 that the asset file was successfully offloaded, and that the portable electronic device 14 may delete its local copy of the asset file.

[0042] When the fixed-length unique identifiers do not match (at block 412) or the manifest digital signature is not valid (at block 414), this may indicate that the asset file was not successfully offloaded, or may have been altered or corrupted. In such case, the electronic processor 205 transmits, via the network interface 215, a denial of the deletion request to the portable electronic device 14. The denial may include a request that the portable electronic device 14 retry the offload process.

[0043] It may be desirable to re-validate an offloaded asset at a later date. For example, a prosecuting attorney preparing for trial may wish to authenticate an asset

to be used for evidence at the trial. In another example, an officer may want to double check that a critical asset file was offloaded successfully before deleting the locally-stored asset file. Accordingly, FIG. 5 illustrates an exemplary sub-method 500 of maintaining chain of custody for assets offloaded from the portable electronic device.

[0044] At block 502, the electronic processor 205, receives, via the network interface 215, a re-validation request. The re-validation request may be received from the portable electronic device 14, or it may be received from another system (for example, a computer at a law enforcement agency or district attorney's office). The re-validation request includes at least one asset identifier (one for each asset file being re-validated), a fixed-length unique identifier for each asset file, and the manifest digital signature originally used when offloading the asset file.

[0045] In response to receiving the re-validation request, the electronic processor 205 determines, as described above in relation to the method 400, at least one asset file fixed-length unique identifier (one for each asset file being re-validated), at block 504. If the asset file is not stored locally in asset management controller 16 or the asset management database 18, the electronic processor 205 retrieves the asset file from the data warehouse before determining the at least one asset file fixed-length unique identifier.

[0046] At block 506, the electronic processor 205 compares the asset file fixed-length unique identifier determined at block 504 with the fixed-length unique identifier received at block 502. At block 508, the electronic processor 205 validates the manifest digital signature, as described above in relation to the method 400. At block 514, when the fixed-length identifiers match (at block 510) and the manifest digital signature block is valid (at block 512), the electronic processor 205 transmits, via the network interface 215, a validation message. The validation message indicates, to the device that requested the re-validation, that the asset file retrieved from the data warehouse is identical to the asset file originally captured by the portable electronic device 14.

[0047] At block 516, when the fixed-length identifiers do not match (at block 510) or the manifest digital signature block is not valid (at block 512), the electronic processor 205 transmits, via the network interface 215, a validation failure message.

The validation failure message indicates, to the device that requested the re-validation, that the asset file retrieved from the data warehouse does not match the asset file originally captured by the portable electronic device 14.

[0048] In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present teachings.

[0049] The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

[0050] Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms “comprises,” “comprising,” “has,” “having,” “includes,” “including,” “contains,” “containing” or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises, has, includes, contains a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element preceded by “comprises ...a,” “has ...a,” “includes ...a,” or “contains ...a” does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises, has, includes, contains the element. The terms “a” and “an” are defined as one or more unless explicitly stated otherwise herein. The terms “substantially,” “essentially,” “approximately,” “about” or any other version thereof, are defined as being close to as understood by one of ordinary skill in the art, and in one non-limiting embodiment the term is defined to be

within 10%, in another embodiment within 5%, in another embodiment within 1% and in another embodiment within 0.5%. The term “coupled” as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is “configured” in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

[0051] It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or “processing devices”) such as microprocessors, digital signal processors, customized processors and field programmable gate arrays (FPGAs) and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and/or apparatus described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used.

[0052] Moreover, an embodiment can be implemented as a computer-readable storage medium having computer readable code stored thereon for programming a computer (e.g., comprising a processor) to perform a method as described and claimed herein. Examples of such computer-readable storage mediums include, but are not limited to, a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill, notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

[0053] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding

that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

Claims

We claim:

1. A system for maintaining chain of custody for assets offloaded from a portable electronic device, the system comprising:

an asset management controller including

a network interface; and

an electronic processor coupled to the network interface and configured to

receive, from the portable electronic device via the network interface, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier associated with the at least one asset identifier, and a manifest digital signature;

transmit, to the portable electronic device via the network interface, at least one storage message based on the asset manifest;

receive, from the portable electronic device via the network interface, an upload completion message;

retrieve, from a data warehouse via the network interface, at least one asset file;

determine, for the at least one asset file, at least one asset file fixed-length unique identifier;

determine whether the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier;

determine whether the manifest digital signature is valid; and

transmit, via the network interface, an asset deletion permission message when the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, and the manifest digital signature is valid.

2. The system of claim 1, wherein the upload completion message includes a request to delete assets stored in a local memory of the portable electronic device.
3. The system of claim 1, wherein the electronic processor is further configured to
 - receive, via the network interface, a re-validation request including the at least one asset identifier, the at least one fixed-length unique identifier and the manifest digital signature;
 - in response to receiving the re-validation request,
 - determine at least one asset file fixed-length unique identifier based on the at least one asset identifier;
 - compare the at least one fixed-length unique identifier with the at least one asset file fixed-length unique identifier,
 - validate the manifest digital signature; and
 - when the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, and the manifest digital signature is valid,
 - transmit, via the network interface, a validation message.
4. The system of claim 1, wherein the at least one fixed-length unique identifier and the at least one asset file fixed-length unique identifier are SHA256 hash values.
5. The system of claim 1, wherein the manifest digital signature is generated from a private key known only to the portable electronic device.

6. The system of claim 1, wherein the electronic processor is further configured to
- receive, from the portable electronic device via the network interface, a digital certificate including a public key;
 - validate the digital certificate; and
 - validate the manifest digital signature based on the public key.
7. The system of claim 1, wherein the portable electronic device is a body-worn camera.

8. A method for maintaining chain of custody for assets offloaded from a portable electronic device, the method comprising:

receiving, by an electronic processor, via a network interface coupled to the electronic processor, from the portable electronic device, an asset manifest including at least one asset identifier, at least one fixed-length unique identifier associated with the at least one asset identifier, and a manifest digital signature;

transmitting, by the electronic processor via the network interface, to the portable electronic device, at least one storage message based on the asset manifest;

receiving, by the electronic processor via the network interface, from the portable electronic device, an upload completion message;

retrieving, by the electronic processor via the network interface, at least one asset file from a data warehouse;

determining, by the electronic processor, for the at least one asset file, at least one asset file fixed-length unique identifier;

determining, by the electronic processor, whether the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier;

determining, by the electronic processor, whether the manifest digital signature is valid; and

transmitting, by the electronic processor via the network interface, an asset deletion permission message when the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, and the manifest digital signature is valid.

9. The method of claim 8, wherein the upload completion message includes a request to delete assets stored in a local memory of the portable electronic device.

10. The method of claim 8, further comprising:

receiving, by the electronic processor via the network interface, a re-validation request including the at least one asset identifier, the at least one fixed-length unique identifier and the manifest digital signature;

in response to receiving the re-validation request,

determining, by the electronic processor, at least one asset file fixed-length unique identifier based on the at least one asset identifier;

comparing, by the electronic processor, the at least one fixed-length unique identifier with the at least one asset file fixed-length unique identifier,

validating, by the electronic processor, the manifest digital signature;

and

when the at least one fixed-length unique identifier matches the at least one asset file fixed-length unique identifier, and the manifest digital signature is valid,

transmitting, by the electronic processor via the network interface, a validation message.

11. The method of claim 8, wherein the at least one fixed-length unique identifier and the at least one asset file fixed-length unique identifier are SHA256 hash values.

12. The method of claim 8, wherein the manifest digital signature is generated from a private key known only to the portable electronic device.

13. The method of claim 8, further comprising:
 - receiving, by the electronic processor via the network interface, from the portable electronic device, a digital certificate including a public key;
 - validating, by the electronic processor, the digital certificate; and
 - validating, by the electronic processor, the manifest digital signature based on the public key.
14. The method of claim 8, wherein the portable electronic device is a body-worn camera.

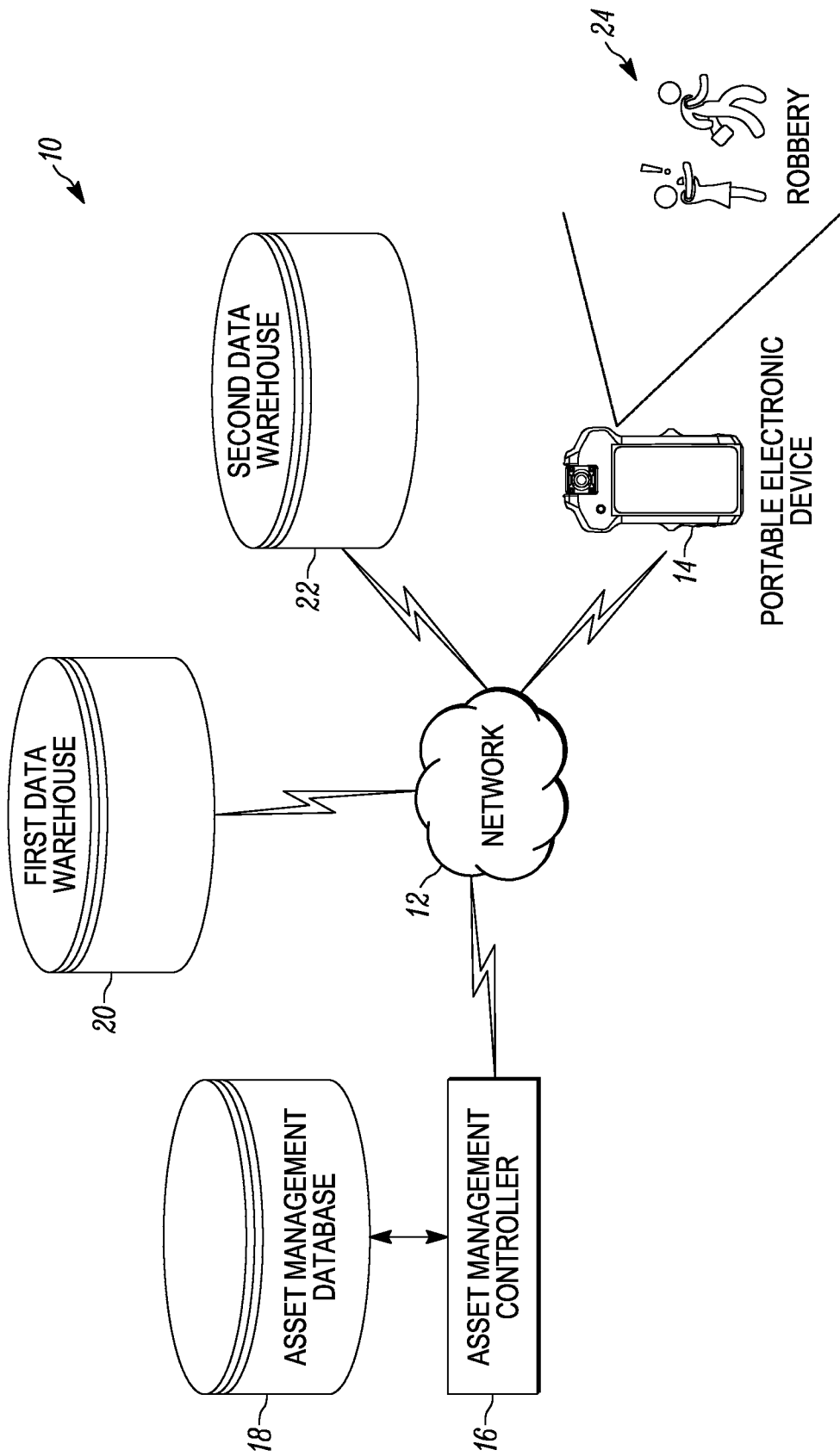


FIG. 1

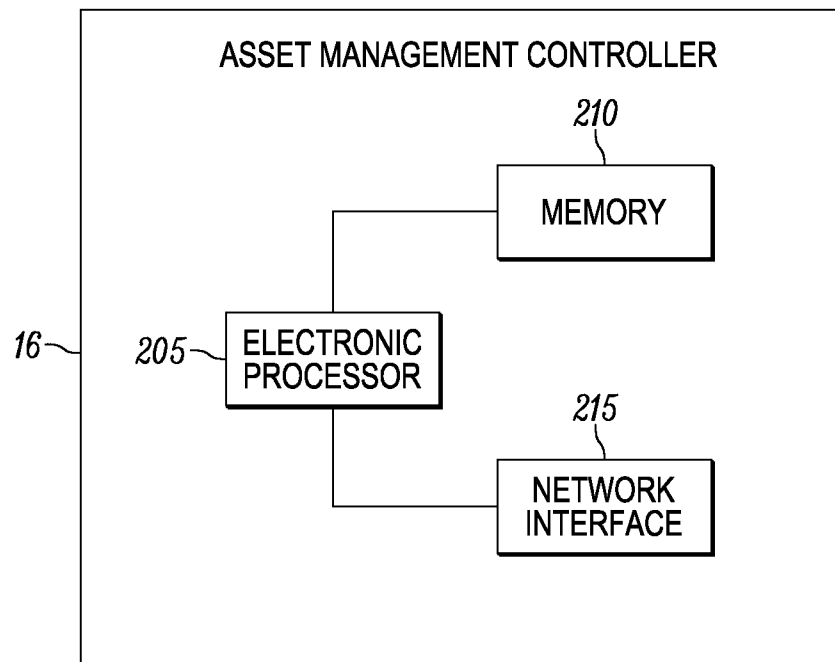
2/5

FIG. 2

3/5

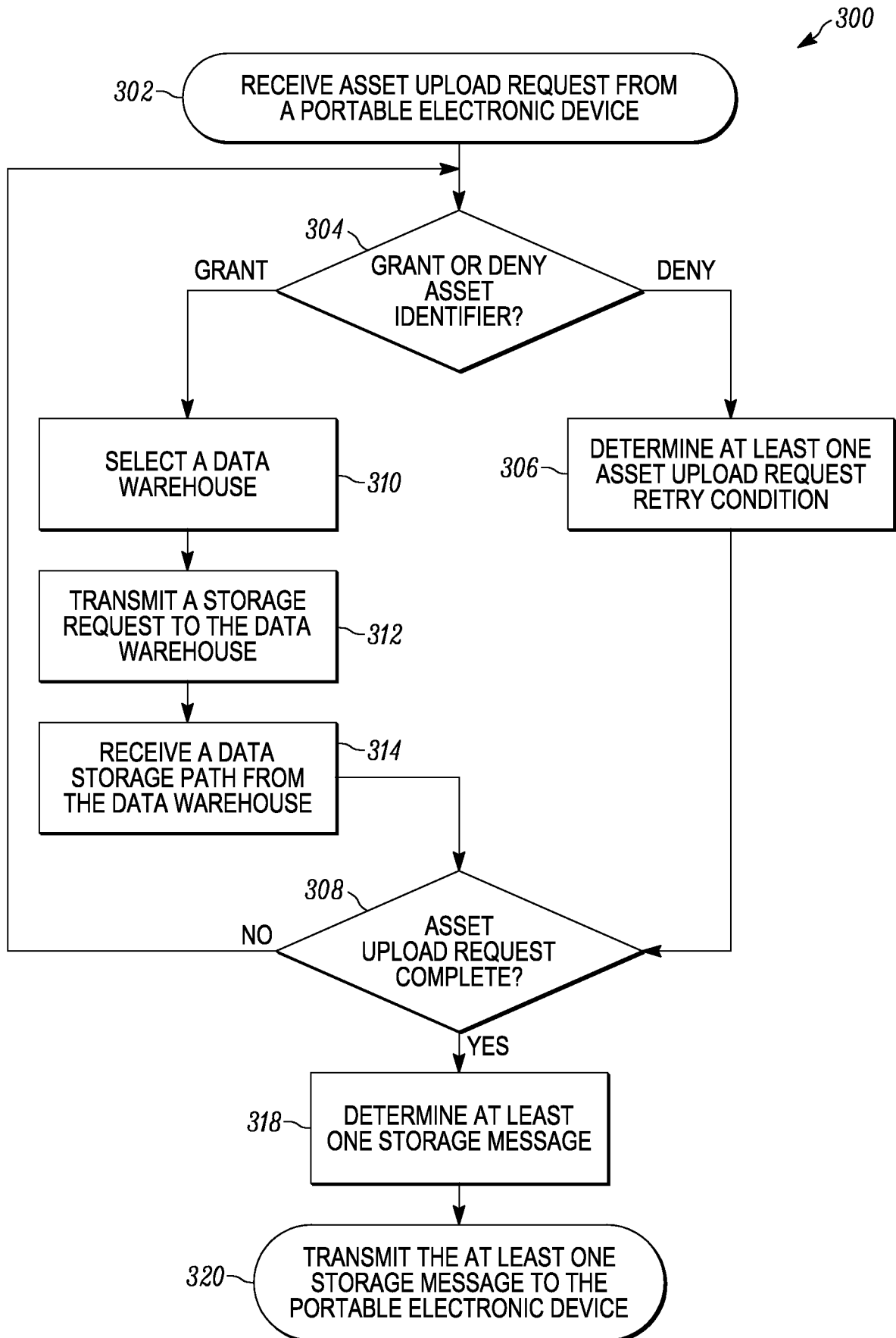


FIG. 3

4/5

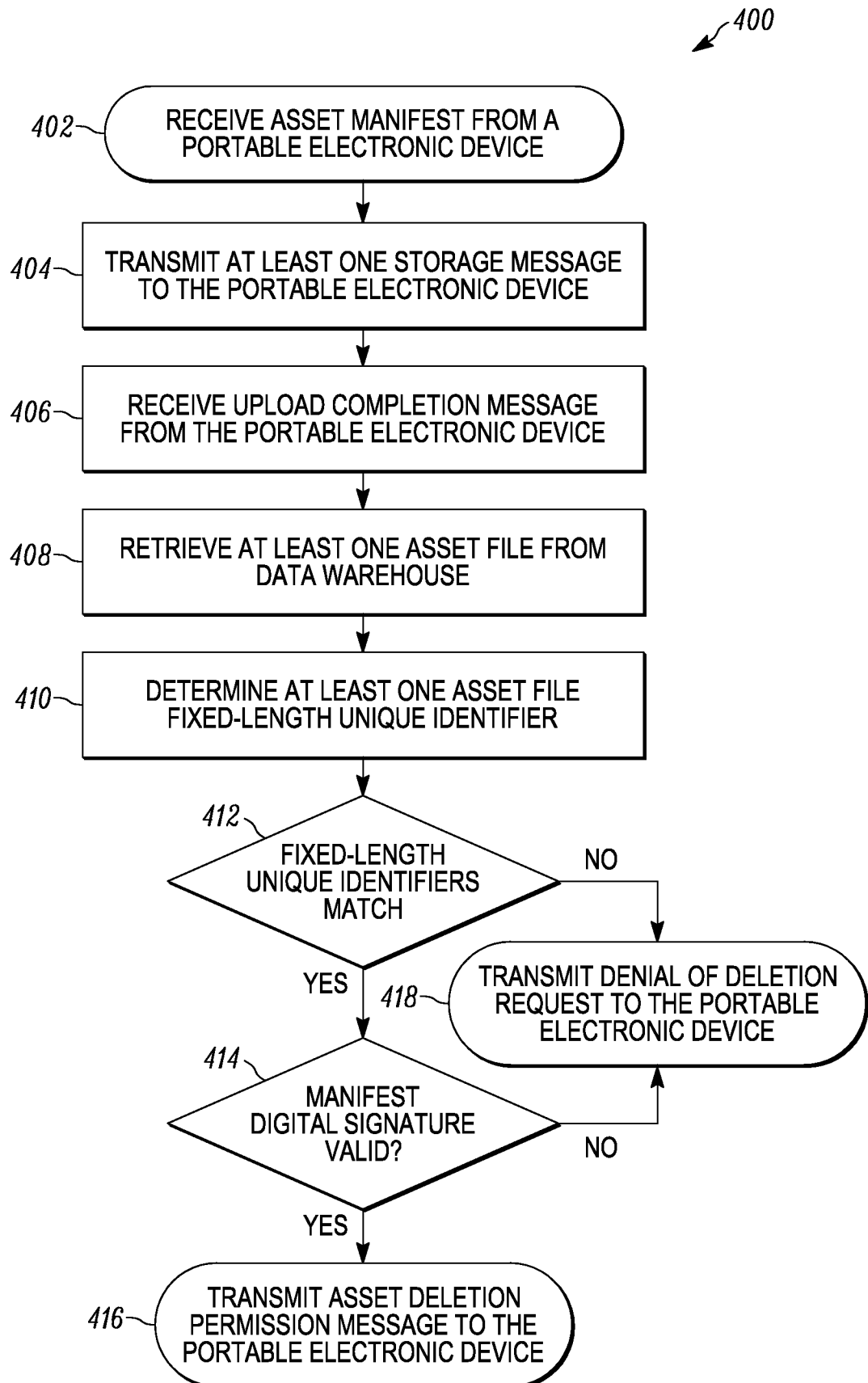


FIG. 4

5/5

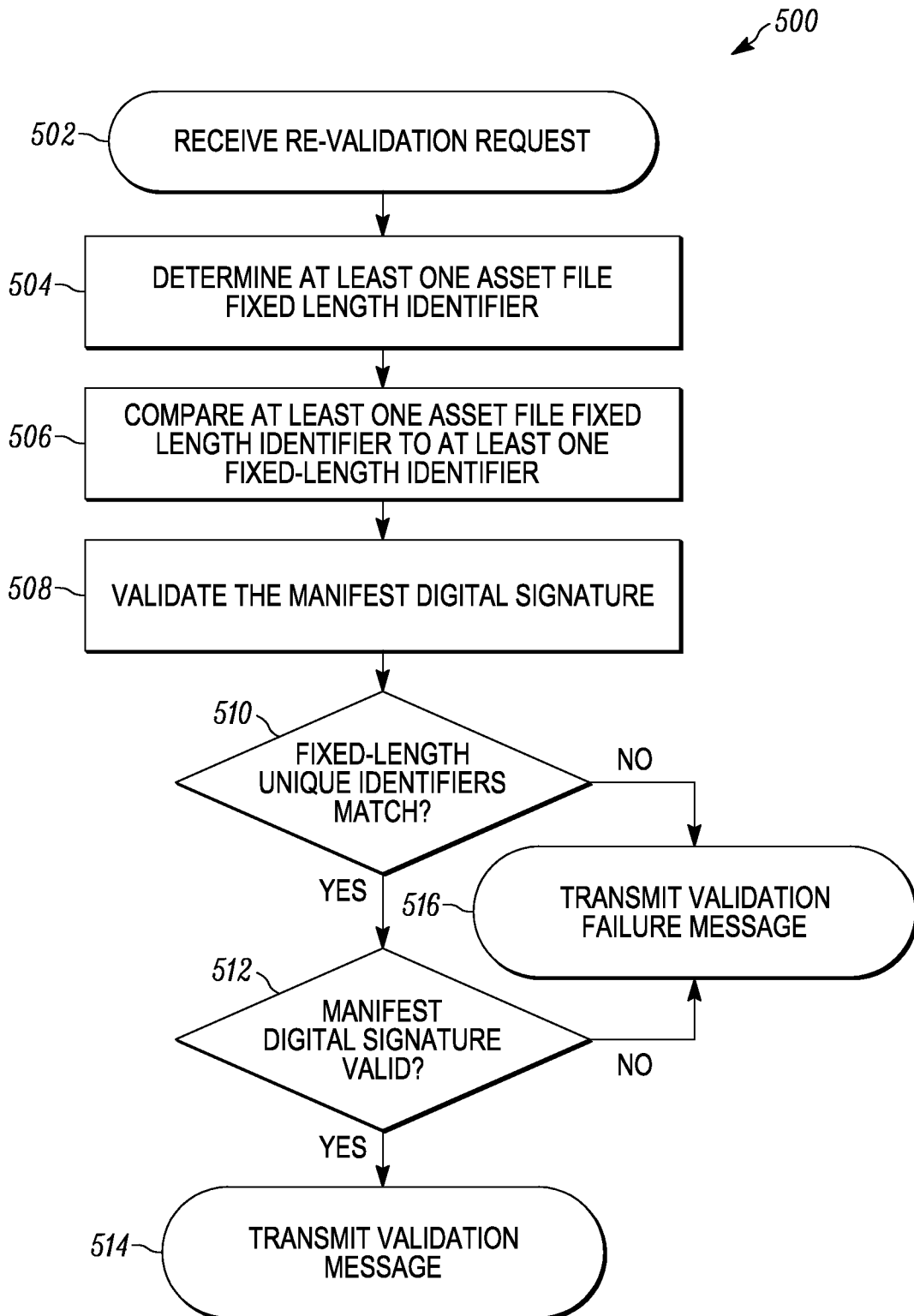


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/PL2016/050022

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q10/00 G06Q50/26
ADD.

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)
G06Q

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013/098476 A1 (P2S MEDIA GROUP OY [FI]) 4 July 2013 (2013-07-04) abstract; figures 1,2,4,5 page 5, line 27 - page 8, line 11 -----	1-14
X	US 2013/039542 A1 (GUZIK THOMAS [US]) 14 February 2013 (2013-02-14) abstract; figures 1,3,4 paragraph [0023] - paragraph [0030] paragraph [0060] - paragraph [0061] -----	1-14



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 another 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

10 August 2016

Date of mailing of the international search report

23/08/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Peller, Ingrid

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/PL2016/050022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013098476 A1	04-07-2013	EP 2798819 A1	05-11-2014
		US 2015058370 A1	26-02-2015
		WO 2013098476 A1	04-07-2013

US 2013039542 A1	14-02-2013	US 2013039542 A1	14-02-2013
		WO 2013059255 A1	25-04-2013
