(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2018 (29.03.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/057404 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 21/10* (2013.01)

(21) International Application Number:
PCT/US2017/051682

(22) International Filing Date:
15 September 2017 (15.09.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/274,367 23 September 2016 (23.09.2016) US

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventor: **LIN, Eugene Seichi**; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: **MINHAS, Sandip S.** et al.; Microsoft Technology Licensing, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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.

WO 2018/057404 A1

(54) Title: TOKENIZED LINKS WITH GRANULAR PERMISSIONS

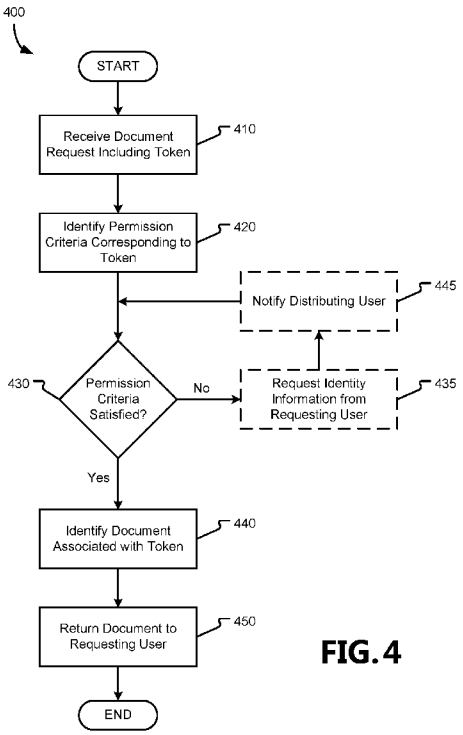


FIG. 4

(57) Abstract: Systems and methods for generating and handling tokenized links pointing to web-accessible files are provided herein. The tokenized link obscures the filepath of the file and is associated with a permission scope that consists of a set of criteria for evaluating conditions for access to the file. The link may be freely shared and still provide access restrictions within a domain to the linked file without needing to modify the permissions for the file itself. A user with access to the file may thus freely share the link with other users, who may in turn share the link with yet other users, and be assured that only authorized users will gain access to the file. The tokenized links thereby improve the security of the files, the user experience of the distributing and receiving users, and the functionality of the devices using the tokenized links.

[Continued on next page]

(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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

TOKENIZED LINKS WITH GRANULAR PERMISSIONS

BACKGROUND

[0001] When sharing a document among collaborators, users may either restrict access to the document itself or its filepath. Neither of these options provide for the flexible sharing and robust security that users desire. Restricting access to the document itself requires that a distributing user manually input the identities of authorized users (i.e., those users who are granted access to read or write to the document), but the document itself may still be visible (albeit not accessible) to unauthorized users. Providing a hidden filepath, in contrast, may prevent unauthorized users from coming across documents that are not accessible to them, but if a link is inadvertently shared, the security of the document will have been compromised. Alternatively, links may be limited in their accessibility to a domain, but a domain may include persons who are part of an organization, but lack the need-to-know, which will still require the document to be access restricted or the link to be not shared with those persons to maintain proper security within the domain.

SUMMARY

[0002] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description section. This summary is not intended to identify all key or essential features of the claimed subject matter, nor is it intended as an aid in determining the scope of the claimed subject matter.

[0003] Systems and methods for providing tokenized links are provided herein. A link that is tokenized points to a document and is associated with a permission scope that consists of a set of criteria for evaluating conditions at the time the link is accessed (e.g., identity, group membership, device state, time/date) to determine whether the user is granted access to the linked document. The link may be freely shared and still provide access restrictions within a domain to the linked document without needing to modify the permissions for the document itself. A user with access to the document may thus freely share the link (e.g., via emails, Instant Messages, forum posts) with other users, who may in turn share the link with yet other users, and be assured that only authorized users will gain access to the document.

[0004] The computing device hosting the linked-to file, such as a document server, receives the request for a document that includes the token for the document from a device associated with a requesting user. The hosting device uses the token and the identity of the requesting user to determine whether the permission criteria set for the link are satisfied by

the requesting user. In response to the permission criteria being satisfied, the document is provided to the requesting user, otherwise the hosting device may query the requesting user for additional identifying information or may deny the request for the document. By verifying permissions relative to the tokenized link, rather than the document itself, distributing users may create multiple sharing profiles for a single document that obscure the location and identity of the document itself to unauthorized parties, provide greater flexibility in sharing the documents, and may require a lower expenditure of processing resources to handle, thus improving the functionality of the computer devices involved.

[0005] Examples are implemented as a computer process, a computing system, or as an article of manufacture such as a device, computer program product, or computer readable medium. According to an aspect, the computer program product is a computer storage medium readable by a computer system and encoding a computer program comprising instructions for executing a computer process.

[0006] The details of one or more aspects are set forth in the accompanying drawings and description below. Other features and advantages will be apparent from a reading of the following detailed description and a review of the associated drawings. It is to be understood that the following detailed description is explanatory only and is not restrictive of the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate various aspects. In the drawings:

FIGURE 1 illustrates an example environment in which the present disclosure may be practiced;

FIGURE 2 is a block diagram of a link tokenizer;

FIGURE 3 is a flow chart showing general stages involved in an example method for providing a tokenized link for a document;

FIGURE 4 is a flow chart showing general stages involved in an example method for requesting a document via a tokenized link;

FIGURE 5 is a block diagram illustrating example physical components of a computing device;

FIGURES 6A and **6B** are block diagrams of a mobile computing device; and

FIGURE 7 is a block diagram of a distributed computing system.

DETAILED DESCRIPTION

[0008] The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description refers to the same or similar elements. While examples may be described, modifications, adaptations, and other implementations are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the drawings, and the methods described herein may be modified by substituting, reordering, or adding stages to the disclosed methods. Accordingly, the following detailed description is not limiting, but instead, the proper scope is defined by the appended claims. Examples may take the form of a hardware implementation, or an entirely software implementation, or an implementation combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

[0009] Systems and methods for providing tokenized links are provided herein. A tokenized link points to a document and is associated with a permission scope that includes of a set of criteria for evaluating conditions at the time the link is accessed (e.g., identity, group membership, device state, time/date) to determine whether the user is granted access to the linked document. The link may be freely shared and still provide access restrictions within a domain to the linked document without modifying the permissions for the document itself. A user with access to the document may thus freely share the link (e.g., via emails, Instant Messages, forum posts) with other users, who may in turn share the link with yet other users, and be assured that only authorized users will gain access to the document.

[0010] The computing device hosting the linked-to file receives the request for a document that includes the token for the document from a device associated with a requesting user. The hosting device uses the token and the identity of the requesting user to determine whether the permission criteria set for the link are satisfied by the requesting user. In response to the permission criteria being satisfied, the document is provided to the requesting user, otherwise the hosting device may query the requesting user for additional identifying information or may deny the request for the document. By verifying permissions relative to the tokenized link, rather than the document itself, distributing users may create multiple sharing profiles for a single document that obscure the location and identity of the document itself to unauthorized parties, thereby providing greater flexibility in sharing the documents, and lowering the expenditure of processing resources to handle, thus improving the functionality of the computer devices involved.

[0011] **FIGURE 1** illustrates an example environment **100** in which the present disclosure may be practiced. As illustrated, a distributing device **110** is in communication with a first requesting device **120a** (generally, requesting device **120**), a document server **130** hosting at least one document **140**, and an identity service **150**. The first requesting device **120a** is in communication with the distributing device **110**, the document server **130**, the identity service **150**, and may be in communication with a second requesting device **120b**, which in turn is in communication with the identity service **150**, and may (or may not) be in communication with the distributing device **110** or the document server **130**. As will be appreciated, the devices illustrated in **FIGURE 1** are provided as examples, and more or fewer of the identified devices may be present in various aspects.

[0012] The distributing device **110**, the requesting device **120**, document server **130**, and identity service **150** are illustrative of a multitude of computing systems including, without limitation, desktop computer systems, wired and wireless computing systems, mobile computing systems (e.g., mobile telephones, netbooks, tablet or slate type computers, notebook computers, and laptop computers), hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, printers, and mainframe computers. The hardware of these computing systems is discussed in greater detail in regard to **FIGURES 5**, **6A**, **6B**, and 7. Distributing device **110** and requesting devices **120** are operated by users, who may be humans or automated systems (e.g., "bots") that access and share document **140** stored on document servers **130**. In various aspects, the distributing device **110**, the requesting device **120**, the document server **130**, and the identity service **150** may be accessed by a user or each other locally and/or by a network, which may include the Internet, a Local Area Network (LAN), a private distributed network for an entity (e.g., a company, a university, a government agency), a wireless *ad hoc* network, a Virtual Private Network (VPN) or other direct data link (e.g., Bluetooth connection, a direct wired link).

[0013] In various aspects, the document **140** for which the tokenized link is generated includes any type of computer readable file that the distributing user wishes to share over a network. Example file types for the document include, but are not limited to: word processing documents, spreadsheets, databases, presentations, canvas files, images, sound files, videos, archives, webpages, executables, libraries, binaries, computer aided design files, certificates, and portions thereof.

[0014] The distributing device **110** is used by a user (a distributing user) to request a tokenized link for a document **140** stored on the document server **130** which is then shared

with one or more requesting device **120** to enable the user (a receiving or requesting user) of that device to request the document **140** via the tokenized link from the document server **130** or forward the tokenized link to one or more additional requesting devices **120** to allow those users to forward the tokenized link or request the document **140**. In various aspects, the distributing device **110** may also be a requesting device **120**, such as, for example, when the distributing user attempts to request the document **140** via the tokenized link.

[0015] In various aspects, the document server **130** is provided by the distributing device **110** or by a separate computing device. The document server **130** stores the documents **140** for which tokenized links are created. The tokenized link points to the document server **130** and includes a token that is interpretable by the document server **130** to retrieve the linked-to document **140** when the requesting user is authorized to access that document **140**. In various aspects, the document server **130** provides a link tokenizer **200** (discussed in greater detail in regard to **FIGURE 2**) to create the tokens used in the links and to interpret those tokens and identifying information for the requesting users against sharing criteria set by the distributing user before sharing the linked-to document **140** to the requesting devices **120**.

[0016] The users of the distributing device **110** and each requesting device **120** are authenticated by one or more identity services **150**. The identity service **150** is operable to allow the users to log into the distributing device **110** or requesting device **120** as well as third party services (e.g., an online email application, a social networking website, a Virtual Private Network (VPN)). A given user may log into multiple identity services **150** via a single device, which will provide various identities for the user. For example, a user may log into a personal device's operating system as "John Doe", and into an online email application as "DoeJohn2000@example.com"; the user is still the same person, but each identity service **150** may associate the user with different preferences, historical use data, and security settings. An identity service **150** logs the users into various systems by the use of a shared secret associated with a username and/or domain name, such as, for example, a password, a biometric marker, or an access token. When a user provides the shared secret held by the identity service **150**, the user is logged into the identity service **150** will be provided with an authorization token to use the device, access files, or use a service that has its access controlled by the identity service **150**.

[0017] In various aspects, an identity service **150** runs on a distributing device **110** or a requesting device **120**, thus allowing local access to the devices when network connectivity is not available to a remote identity service **150**. In additional aspects, an

identity service **150** runs on the document server **130** or in a network environment hosting the document server **130**. In yet other aspects, the identity service **150** is a third-party service running on a device that is not controlled by the distributing, requesting, or receiving users or the host of the document **140**, which provides access control for one or more network environments or services.

[0018] **FIGURE 2** is a block diagram of a link tokenizer **200**. In various aspects, the link tokenizer **200** is provided by the document server **130** or another device in communication with the document server **130** to create tokenized links and to control access to the documents **140** linked to by the tokenized links. The link tokenizer **200** provides or is in communication with: a token generator **210**, operable to produce a token for a document **140** associated with permission criteria; a document storage **220**, in which the document **140** is stored and from which the document **140** is accessible; a linking database **230**, operable to store associations between token, the document **140**, and the permission criteria; and a permission checker **240**, operable to evaluate requests that include tokens to provide the document **140** to users who satisfy the permission criteria.

[0019] The token generator **210** is in communication with the distributing device **110**, the document storage **220**, and the linking database **230**. The distributing device **110** communicates the document **140** for which a token is to be generated and the permission criteria to the token generator **210**, which produces a token for the document **140** and transmits the token to the distributing device **110** for use in a tokenized link. The token generator **210** transmits the identity of the document and/or its filepath in the document storage **220**, the permissions criteria, and the token to the linking database **230**, which associates these data and stores them for later lookup and cross-reference.

[0020] The permission checker **240** is in communication with requesting devices **120** using the tokenized links to request documents **140**, the linking database **230**, and the document storage **220**. When a request for the document **140** is received from a requesting device **120**, the permission checker **240** extracts the token from the request and queries the linking database **230** for the identity and/or filepath of the associated document **140** and the permission criteria for the tokenized link. The permission checker **240** compares the identity information from the requesting device **120**, time at which the request was received, etc., to the permission criteria to determine whether the request satisfies the permission criteria. When the request does not satisfy the permission criteria, the permission checker **240** is operable to transmit a request to the requesting device **120** to provide identifying information that will satisfy the permission criteria or a message indicating that the

requesting user is not authorized to access the document **140** via the tokenized link. When the request does satisfy the permission criteria, the permission checker **240** is operable to signal the document storage **220** to retrieve the linked-to document **140** and transmit it to the authorized requesting device **120**.

[0021] **FIGURE 3** is a flow chart showing general stages involved in an example method **300** for providing a tokenized link for a document **140**. Method **300** begins when a request for link tokenization for a document **140** is received at OPERATION **310** from a distributing device **110**.

[0022] The method proceeds to OPERATION **320**, where the permission criteria for which users are allowed to follow the tokenized link to the document **140** are received. In various aspects, the permissions criteria are specified in conjunction with the initial request received at OPERATION **310**, while in other aspects, the permissions criteria may be adjusted at a later time before or after the tokenized link has been generated. In some aspects, the permission criteria are based on the identity information for the distributing user, while in other aspects, the distributing user may specify various identity information, time windows, and access rights (e.g., read, read/write) for permission criteria. For example, the distributing user may specify that the tokenized link will only be available for a set period of time, to requesting users from a specified domain or subset of a domain (e.g., employees of Acme, Inc., employees of Acme, Inc. who are also part of the human resources department), to requesting users using permitted identity services **150** (or not using forbidden identity services **150**), among other conditions. In yet other aspects, the permission criteria may be set to null, so that any user in possession of the tokenized link can access the document **140**.

[0023] At OPERATION **330** a token is created for use in the tokenized link. The token is a value that is sufficiently random to prevent a user from guessing the identity of the document **140** linked to from its format, and distinct in its value from other tokens already in use. In various aspects, the token may be created based on a hashing of the filepath of the document **140** and a nonce (e.g., a timestamp) to ensure that each token generated is unique or at least statistically unlikely to be reused within a given link tokenizer **200**. A hash function yields a one-way encryption of data, which may be done according to various algorithms known to those of ordinary skill in the art (SHA-2, SHA256, MD5, BLAKE2, Keccak, GOST, etc.). In other aspects, the token may be an incremented counter that is updated for each document **140** for which a tokenized link is requested.

[0024] Method **300** proceeds to OPERATION **340** where the document **140** is associated with the token, and the token is associated with the permission criteria. These associations are saved for accessing the document **140** via the tokenized link, which is discussed in greater detail in regard to **FIGURE 4**. The associations may be stored in a database, such as the linking database **230** of the link tokenizer **200**, or may be stored within a domain name server of the network environment in which the document server **130** is provided to evaluate and redirect the requests using the tokenized link to access the document **140**.

[0025] At OPERATION **350** the token is returned to the distributing device **110** for incorporation into the tokenized link. In various aspects, the tokenized link points to the document server **130** or the host for the network environment in which the document server **130** is provided. The distributing device **110** may, in various aspects, include the token as part of the path of the URL (Uniform Resource Locator) for the tokenized link or include the token as a query for the URL. Method **300** then concludes.

[0026] **FIGURE 4** is a flow chart showing general stages involved in an example method **400** for requesting a document **140** via a tokenized link. Method **400** begins at OPERATION **410** in response to the document server **130** receiving a document request that uses a tokenized link, including a token for a linked-to document **140**. The token is extracted from the tokenized link and used at OPERATION **420** to retrieve the permissions criteria set for sharing the document **140**, and method **400** proceeds to DECISION **430**. In various aspects, the token is used as a key value to retrieve the permission criteria from a linking database **230**.

[0027] At DECISION **430** it is determined whether the permission criteria are satisfied. In response to determining that the permission criteria are satisfied, method **400** will proceed to OPERATION **440**. In response to determining that the permission criteria are not satisfied, method **400** may optionally proceed to OPERATION **435** or OPERATION **445**, or may wait until the permission criteria are satisfied.

[0028] In various aspects, the permission criteria include a time range in which the tokenized link is valid and the permission criteria will be determined to not be satisfied when the request is received outside of the specified time range. For example, a distributing user may specify that a given document **140** will be available from Tuesday until Friday, and any requesting user that uses the tokenized link before Tuesday or after Friday will be determined to not satisfy the permission criteria for the time range, whereas any requesting

user that uses the tokenized link between Tuesday and Friday will be determined to satisfy the permission criteria for the time range.

[0029] When the permission criteria include a domain for which the tokenized link is valid (or invalid), the domain information of the requesting user are compared to the permission criteria. The domain information may be looked up from a domain controller and/or included in the request or when establishing the communications session between the requesting device **120** and the document server **130** (e.g., via a handshake procedure). For example, a distributing user may have specified that only users from domain X or verified by a given identity service **150** as belonging to domain X may access the document **140** via the tokenized link, and accordingly requesting users from those domains are determined to satisfy the permission criteria. In another example, a distributing user may have specified that users from domain X or verified by a given identity service **150** as belonging to domain X are forbidden from accessing the document **140** via the tokenized link, and accordingly requesting users from those forbidden domains are determined to not satisfy the permission criteria.

[0030] The permission criteria may also specify specific persons who are allowed or forbidden from using the tokenized link to access the document **140**. The user identities for allowed users will therefore satisfy the permission criteria, and other user identifiers and the user identities for forbidden users will not satisfy the permission criteria. User identities may include usernames, email addresses, telephone numbers, account names/numbers, IP addresses or MAC address associated with a requesting device **120** for a requesting user, and other identifiers.

[0031] In additional aspects, the permission criteria include requirements or conditions related to the requesting device **120** that receives the document **140** from the document server **130**, such as, for example: requiring the requesting device to be managed by the same Information Technology (IT) organization that manages the document server **130** or the distributing device **110**, requiring the requesting device **120** to be connected to a particular network (such as the network managed by the IT organization that manages the document server **130**) locally or remotely (e.g., via a Virtual Private Network), requiring that the identity of the user of the requesting device **120** match a specific list of allowed users (either as a list of individual identities, or a pre-set list (e.g., a distribution list, a directory service group, an access group for a cloud sharing platform). In further aspects, the permission criteria specify identity services **150** from which the user's identity was retrieved as either allowed or denied. For example, an IT administrator, who does not trust

the security policies of a given identity service **150**, sets a permission criteria that prevent users authenticated by a first identity service **150** from using the tokenized link to access the linked document **140**, while allowing users authentication by a second identity service **150** to access the linked document **140** via the tokenized link.

[0032] As will be appreciated, permission criteria may combine time ranges, domains, individuals and/or device conditions for specifying when, how, and by whom a document **140** may be accessed. For example, a distributing user may specifies that John Doe and Jane Doe may each access a given document **140** before the end of the month, but only if they are authenticated by a given identity service **150** as being who they claim to be. Continuing the example, the distributing user may trust the authentication schema used by the given identity service **150** (e.g., a workplace domain controller) to be more up-to-date or secure than a different identity server **150** (e.g., a social media website's access controller).

[0033] At optional OPERATION **435** the document server **130** prompts the requesting user to supply identity information. For example, a requesting user may not be logged into any acceptable identity services **150** (according to the permission criteria), and a prompt will be transmitted to the requesting device **120** to explain to the user to log into an acceptable identity service **150** and reattempt the request via the tokenized link. In another example, a user is logged into an acceptable identity service **150**, but did not supply the identity information to the document server **130**, which queries the requesting device **120** for that information at optional OPERATION **435**. Method **400** may return to DECISION **430** or perform optional OPERATION **445** after optional OPERATION **445**.

[0034] At optional OPERATION **445** the distributing user who requested the tokenized link and set the permission criteria is contacted by the document server **130** in response to receiving a request for the linked-to document **140** that did not satisfy the permission criteria. In various aspects, the distributing user is contacted to prompt the distributing user to modify the permission criteria to allow the request. In other aspects, the distributing user is contacted to alert the distributing user to a number and/or frequency of requests for the document **140** to determine whether to take additional measures to safeguard the document **140** or to distribute the document **140** to a wider audience than the current permission criteria allow. In various aspects, the notification may indicate the user identity of the requesting user whose request did not satisfy the permission criteria, a time the request was made, and may include one or more failing document requests in a single notification.

Method **400** may return to DECISION **430** or perform optional OPERATION **435** after optional OPERATION **445**.

[0035] When the permission criteria are determined to have been satisfied, method **400** proceeds to OPERATION **440**, where the document **140** associated with the token is identified. In various aspects, the token is used as a key value to retrieve the filepath for the document **140** from a linking database **230**. Method **400** then returns the document **140** to the requesting user at OPERATION **450** by transmitting the document **140**, or a portion thereof, to the requesting device **120**. Method **400** then concludes.

[0036] While implementations have been described in the general context of program modules that execute in conjunction with an application program that runs on an operating system on a computer, those skilled in the art will recognize that aspects may also be implemented in combination with other program modules. Generally, program modules include routines, programs, components, data structures, and other types of structures that perform particular tasks or implement particular abstract data types.

[0037] The aspects and functionalities described herein may operate via a multitude of computing systems including, without limitation, desktop computer systems, wired and wireless computing systems, mobile computing systems (e.g., mobile telephones, netbooks, tablet or slate type computers, notebook computers, and laptop computers), hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, and mainframe computers.

[0038] In addition, according to an aspect, the aspects and functionalities described herein operate over distributed systems (e.g., cloud-based computing systems), where application functionality, memory, data storage and retrieval and various processing functions are operated remotely from each other over a distributed computing network, such as the Internet or an intranet. According to an aspect, user interfaces and information of various types are displayed via on-board computing device displays or via remote display units associated with one or more computing devices. For example, user interfaces and information of various types are displayed and interacted with on a wall surface onto which user interfaces and information of various types are projected. Interaction with the multitude of computing systems with which implementations are practiced include, keystroke entry, touch screen entry, voice or other audio entry, gesture entry where an associated computing device is equipped with detection (e.g., camera) functionality for capturing and interpreting user gestures for controlling the functionality of the computing device, and the like.

[0039] **FIGURES 5-7** and the associated descriptions provide a discussion of a variety of operating environments in which examples are practiced. However, the devices and systems illustrated and discussed with respect to **FIGURES 5-7** are for purposes of example and illustration and are not limiting of a vast number of computing device configurations that are utilized for practicing aspects, described herein.

[0040] **FIGURE 5** is a block diagram illustrating physical components (i.e., hardware) of a computing device **500** with which examples of the present disclosure may be practiced. In a basic configuration, the computing device **500** includes at least one processing unit **502** and a system memory **504**. According to an aspect, depending on the configuration and type of computing device, the system memory **504** comprises, but is not limited to, volatile storage (e.g., random access memory), non-volatile storage (e.g., read-only memory), flash memory, or any combination of such memories. According to an aspect, the system memory **504** includes an operating system **505** and one or more program modules **506** suitable for running software applications **550**. According to an aspect, the system memory **504** includes the link tokenizer **200**. The operating system **505**, for example, is suitable for controlling the operation of the computing device **500**. Furthermore, aspects are practiced in conjunction with a graphics library, other operating systems, or any other application program, and are not limited to any particular application or system. This basic configuration is illustrated in **FIGURE 5** by those components within a dashed line **508**. According to an aspect, the computing device **500** has additional features or functionality. For example, according to an aspect, the computing device **500** includes additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape. Such additional storage is illustrated in **FIGURE 5** by a removable storage device **509** and a non-removable storage device **510**.

[0041] As stated above, according to an aspect, a number of program modules and data files are stored in the system memory **504**. While executing on the processing unit **502**, the program modules **506** (e.g., link tokenizer **200**) perform processes including, but not limited to, one or more of the stages of the methods **300** and **400** illustrated in **FIGURES 3** and **4**. According to an aspect, other program modules are used in accordance with examples and include applications such as electronic mail and contacts applications, word processing applications, spreadsheet applications, database applications, slide presentation applications, drawing or computer-aided application programs, etc.

[0042] According to an aspect, the computing device **500** has one or more input device(s) **512** such as a keyboard, a mouse, a pen, a sound input device, a touch input device,

etc. The output device(s) **514** such as a display, speakers, a printer, etc. are also included according to an aspect. The aforementioned devices are examples and others may be used. According to an aspect, the computing device **500** includes one or more communication connections **516** allowing communications with other computing devices **518**. Examples of suitable communication connections **516** include, but are not limited to, radio frequency (RF) transmitter, receiver, and/or transceiver circuitry; universal serial bus (USB), parallel, and/or serial ports.

[0043] The term computer readable media, as used herein, includes computer storage media. Computer storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, or program modules. The system memory **504**, the removable storage device **509**, and the non-removable storage device **510** are all computer storage media examples (i.e., memory storage.) According to an aspect, computer storage media include RAM, ROM, electrically erasable programmable read-only memory (EEPROM), flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other article of manufacture which can be used to store information and which can be accessed by the computing device **500**. According to an aspect, any such computer storage media is part of the computing device **500**. Computer storage media do not include a carrier wave or other propagated data signal.

[0044] According to an aspect, communication media are embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and include any information delivery media. According to an aspect, the term "modulated data signal" describes a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), infrared, and other wireless media.

[0045] **FIGURES 6A** and **6B** illustrate a mobile computing device **600**, for example, a mobile telephone, a smart phone, a tablet personal computer, a laptop computer, and the like, with which aspects may be practiced. With reference to **FIGURE 6A**, an example of a mobile computing device **600** for implementing the aspects is illustrated. In a basic configuration, the mobile computing device **600** is a handheld computer having both input elements and output elements. The mobile computing device **600** typically includes a

display **605** and one or more input buttons **610** that allow the user to enter information into the mobile computing device **600**. According to an aspect, the display **605** of the mobile computing device **600** functions as an input device (e.g., a touch screen display). If included, an optional side input element **615** allows further user input. According to an aspect, the side input element **615** is a rotary switch, a button, or any other type of manual input element. In alternative examples, mobile computing device **600** incorporates more or fewer input elements. For example, the display **605** may not be a touch screen in some examples. In alternative examples, the mobile computing device **600** is a portable phone system, such as a cellular phone. According to an aspect, the mobile computing device **600** includes an optional keypad **635**. According to an aspect, the optional keypad **635** is a physical keypad. According to another aspect, the optional keypad **635** is a "soft" keypad generated on the touch screen display. In various aspects, the output elements include the display **605** for showing a graphical user interface (GUI), a visual indicator **620** (e.g., a light emitting diode), and/or an audio transducer **625** (e.g., a speaker). In some examples, the mobile computing device **600** incorporates a vibration transducer for providing the user with tactile feedback. In yet another example, the mobile computing device **600** incorporates input and/or output ports, such as an audio input (e.g., a microphone jack), an audio output (e.g., a headphone jack), and a video output (e.g., a HDMI port) for sending signals to or receiving signals from an external device. In yet another example, the mobile computing device **600** incorporates peripheral device port **640**, such as an audio input (e.g., a microphone jack), an audio output (e.g., a headphone jack), and a video output (e.g., a HDMI port) for sending signals to or receiving signals from an external device.

[0046] **FIGURE 6B** is a block diagram illustrating the architecture of one example of a mobile computing device. That is, the mobile computing device **600** incorporates a system (i.e., an architecture) **602** to implement some examples. In one example, the system **602** is implemented as a "smart phone" capable of running one or more applications (e.g., browser, e-mail, calendaring, contact managers, messaging clients, games, and media clients/players). In some examples, the system **602** is integrated as a computing device, such as an integrated personal digital assistant (PDA) and wireless phone.

[0047] According to an aspect, one or more application programs **650** are loaded into the memory **662** and run on or in association with the operating system **664**. Examples of the application programs include phone dialer programs, e-mail programs, personal information management (PIM) programs, word processing programs, spreadsheet programs, Internet browser programs, messaging programs, and so forth. The system **602**

also includes a non-volatile storage area **668** within the memory **662**. The non-volatile storage area **668** is used to store persistent information that should not be lost if the system **602** is powered down. The application programs **650** may use and store information in the non-volatile storage area **668**, such as e-mail or other messages used by an e-mail application, and the like. A synchronization application (not shown) also resides on the system **602** and is programmed to interact with a corresponding synchronization application resident on a host computer to keep the information stored in the non-volatile storage area **668** synchronized with corresponding information stored at the host computer. As should be appreciated, other applications may be loaded into the memory **662** and run on the mobile computing device **600**.

[0048] According to an aspect, the system **602** has a power supply **670**, which is implemented as one or more batteries. According to an aspect, the power supply **670** further includes an external power source, such as an AC adapter or a powered docking cradle that supplements or recharges the batteries.

[0049] According to an aspect, the system **602** includes a radio **672** that performs the function of transmitting and receiving radio frequency communications. The radio **672** facilitates wireless connectivity between the system **602** and the "outside world," via a communications carrier or service provider. Transmissions to and from the radio **672** are conducted under control of the operating system **664**. In other words, communications received by the radio **672** may be disseminated to the application programs **650** via the operating system **664**, and vice versa.

[0050] According to an aspect, the visual indicator **620** is used to provide visual notifications and/or an audio interface **674** is used for producing audible notifications via the audio transducer **625**. In the illustrated example, the visual indicator **620** is a light emitting diode (LED) and the audio transducer **625** is a speaker. These devices may be directly coupled to the power supply **670** so that when activated, they remain on for a duration dictated by the notification mechanism even though the processor **660** and other components might shut down for conserving battery power. The LED may be programmed to remain on indefinitely until the user takes action to indicate the powered-on status of the device. The audio interface **674** is used to provide audible signals to and receive audible signals from the user. For example, in addition to being coupled to the audio transducer **625**, the audio interface **674** may also be coupled to a microphone to receive audible input, such as to facilitate a telephone conversation. According to an aspect, the system **602** further

includes a video interface **676** that enables an operation of an on-board camera **630** to record still images, video stream, and the like.

[0051] According to an aspect, a mobile computing device **600** implementing the system **602** has additional features or functionality. For example, the mobile computing device **600** includes additional data storage devices (removable and/or non-removable) such as, magnetic disks, optical disks, or tape. Such additional storage is illustrated in **FIGURE 6B** by the non-volatile storage area **668**.

[0052] According to an aspect, data/information generated or captured by the mobile computing device **600** and stored via the system **602** are stored locally on the mobile computing device **600**, as described above. According to another aspect, the data are stored on any number of storage media that are accessible by the device via the radio **672** or via a wired connection between the mobile computing device **600** and a separate computing device associated with the mobile computing device **600**, for example, a server computer in a distributed computing network, such as the Internet. As should be appreciated such data/information are accessible via the mobile computing device **600** via the radio **672** or via a distributed computing network. Similarly, according to an aspect, such data/information are readily transferred between computing devices for storage and use according to well-known data/information transfer and storage means, including electronic mail and collaborative data/information sharing systems.

[0053] **FIGURE 7** illustrates one example of the architecture of a system for generating and handling tokenized links as described above. Content developed, interacted with, or edited in association with the link tokenizer **200** is enabled to be stored in different communication channels or other storage types. For example, various documents may be stored using a directory service **722**, a web portal **724**, a mailbox service **726**, an instant messaging store **728**, or a social networking site **730**. The link tokenizer **200** is operative to use any of these types of systems or the like for generating and handling tokenized links, as described herein. According to an aspect, a server **720** provides the link tokenizer **200** to clients **705a,b,c**. As one example, the server **720** is a web server providing the link tokenizer **200** over the web. The server **720** provides the link tokenizer **200** over the web to clients **705** through a network **740**. By way of example, the client computing device is implemented and embodied in a personal computer **705a**, a tablet computing device **705b** or a mobile computing device **705c** (e.g., a smart phone), or other computing device. Any of these examples of the client computing device are operable to obtain content from the store **716**.

[0054] Implementations, for example, are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to aspects. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

[0055] The description and illustration of one or more examples provided in this application are not intended to limit or restrict the scope as claimed in any way. The aspects, examples, and details provided in this application are considered sufficient to convey possession and enable others to make and use the best mode. Implementations should not be construed as being limited to any aspect, example, or detail provided in this application. Regardless of whether shown and described in combination or separately, the various features (both structural and methodological) are intended to be selectively included or omitted to produce an example with a particular set of features. Having been provided with the description and illustration of the present application, one skilled in the art may envision variations, modifications, and alternate examples falling within the spirit of the broader aspects of the general inventive concept embodied in this application that do not depart from the broader scope.

CLAIMS

1. A method for improving computer functionality when sharing a document, comprising:

receiving, by a document server, a request for sharing the document via a tokenized link;

receiving, by the document server, permission criteria by which the document is accessible;

creating, by the document server, a token for the document;

saving, by the document server, associations between the token, the document, and the permission criteria;

integrating the token into a link, wherein the link points to the document server; and

transmitting the link to a computing device to enable the computing device to request access to the document from the document server via the link.

2. The method of claim 1, wherein the token is integrated into the link by the document server.

3. The method of claim 1, wherein the token is integrated into the link as a query in a Uniform Resource Locator of the link.

4. The method of claim 1, wherein the permission criteria include:

a domain for a user to access the document via the link;

a time range for the user to access the document via the link;

an identity of the user to access the document via the link;

an identity server from which the user provides the identity to access the document via the link; and

a management organization for the document server by which a user connects the computing device to access the document via the link.

5. The method of claim 1, wherein the link enables a second computing device to request access to the document from the document server without the document server having transmitted the link to the second computing device.

6. The method of claim 1, wherein the document is associated with a second link, the second link associated with second permission criteria.

7. The method of claim 1, wherein the document server is further operable to receive a request for the document via the link and determine whether to share the document based on whether a requesting device using the link satisfies the permission criteria.

8. The method of claim 1, wherein the document server is further operable to receive a request for the document via the link and determine whether to share the document based on whether a user identity of a user making the request satisfies the permission criteria.

9. The method of claim 1, wherein the document server is further operable to receive a request for the document via the link and determine whether to share the document based on whether a time that the request was received satisfies the permission criteria.

10. A method for improving computer functionality when sharing a document, comprising:

receiving, at a document server from a requesting device, a document request including a token;

identifying permission criteria associated with the token;

determining whether the document request satisfies the permission criteria;

in response to determining that the document request satisfies the permission criteria:

identifying a document associated with the token; and

transmitting, from the document server to the requesting device, the document.

11. The method of claim 10, further comprising:

in response to determining that the document request does not satisfy the permission criteria:

transmitting, from the document server to the requesting device, the document a request for user identity information to satisfy the permission criteria.

12. The method of claim 10, wherein the token was previously generated by the document server to share the document in response to a request from a distributing device.

13. The method of claim 12, wherein the requesting device received the token in a link from the distributing device.

14. The method of claim 12, wherein the requesting device received the token from a third device.

15. A system for improving computer functionality when sharing a document, comprising:

a processor; and

a computer readable storage medium embodied as hardware, including instructions that when executed by the processor are operable to enable the system to:

receive a request for sharing the document via a tokenized link;

receive permission criteria by which the document is accessible, wherein the permission criteria include a domain for a user to access the document, a time range for the user to access the document, and requesting device conditions for the requesting device used by the user to access the document;

create a token for the document;

save associations between the token, the document, and the permission criteria;

integrate the token into a link, wherein the link points to the system; and

transmit the link to a first computing device to enable the first computing device to request access to the document from the system via the link and to share the link with a second computing device to enable the second computing device to request access to the document from the system without the system having transmitted the link to the second computing device.

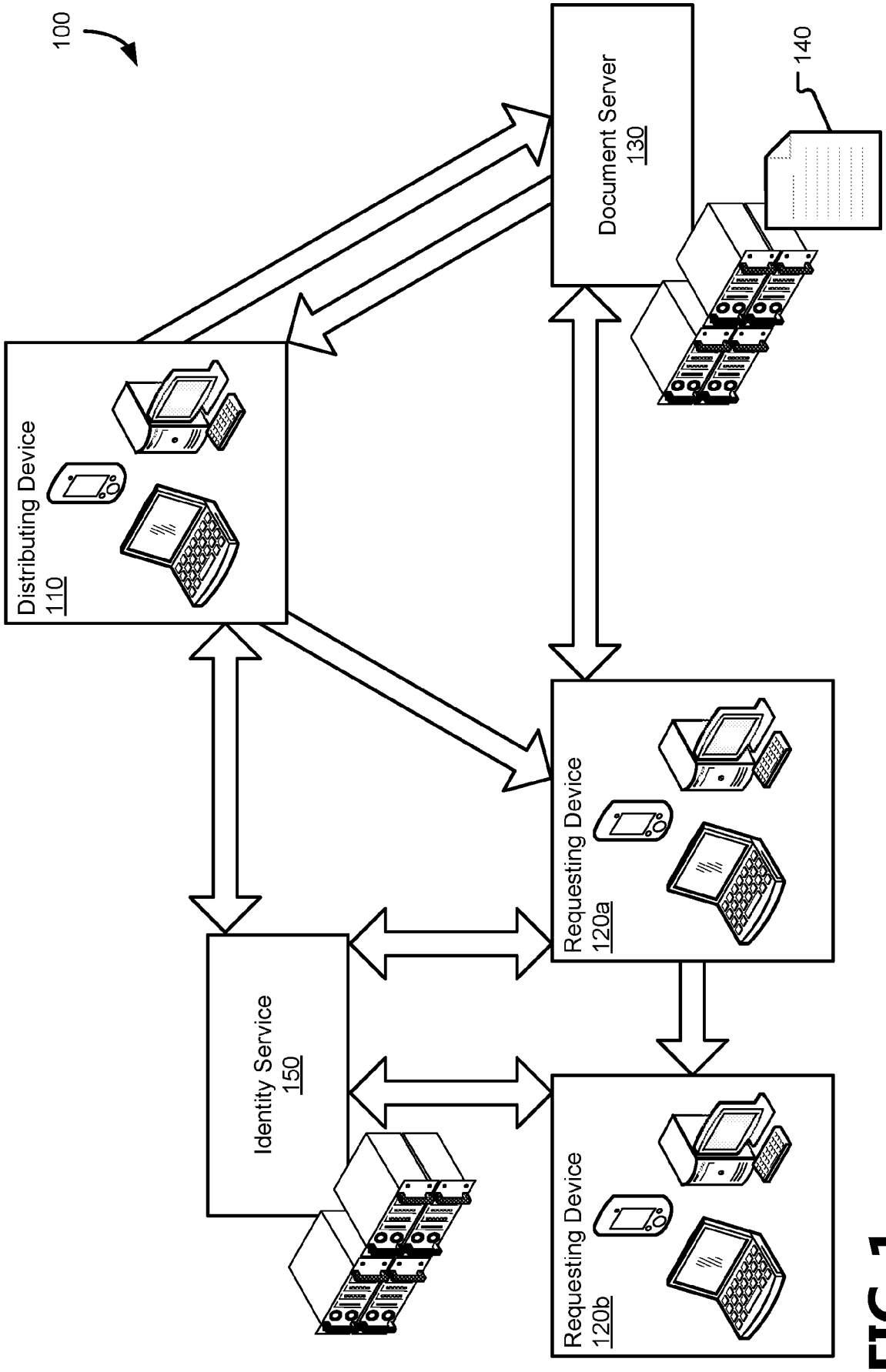

100
Document Server
130
140
Distributing Device
110
Requesting Device
120a
Identity Service
150
Requesting Device
120b

FIG. 1

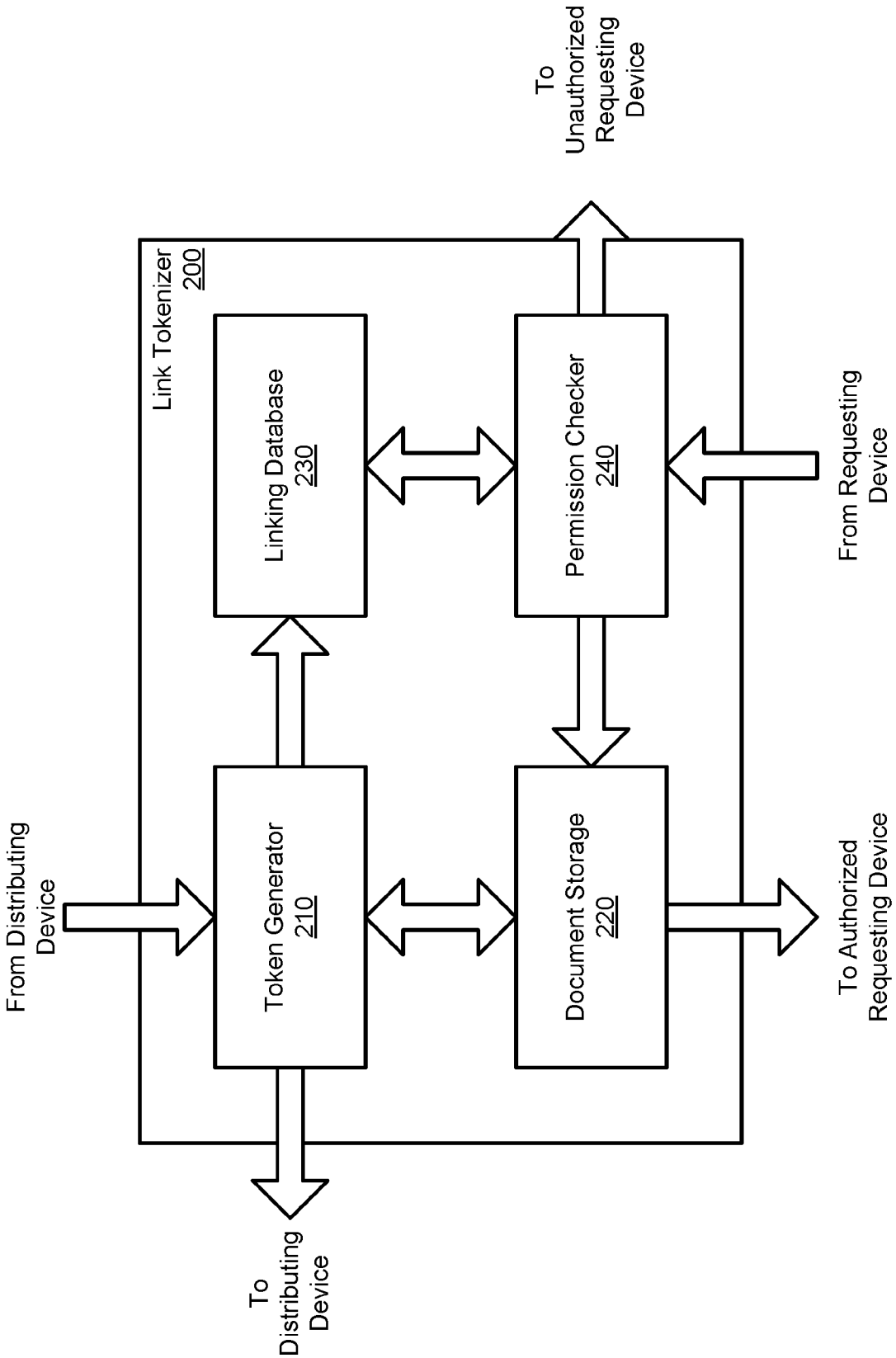

To Unauthorized Requesting Device
Link Tokenizer 200
Linking Database 230
Permission Checker 240
From Requesting Device
From Distributing Device
Token Generator 210
Document Storage 220
To Authorized Requesting Device
To Distributing Device

FIG. 2

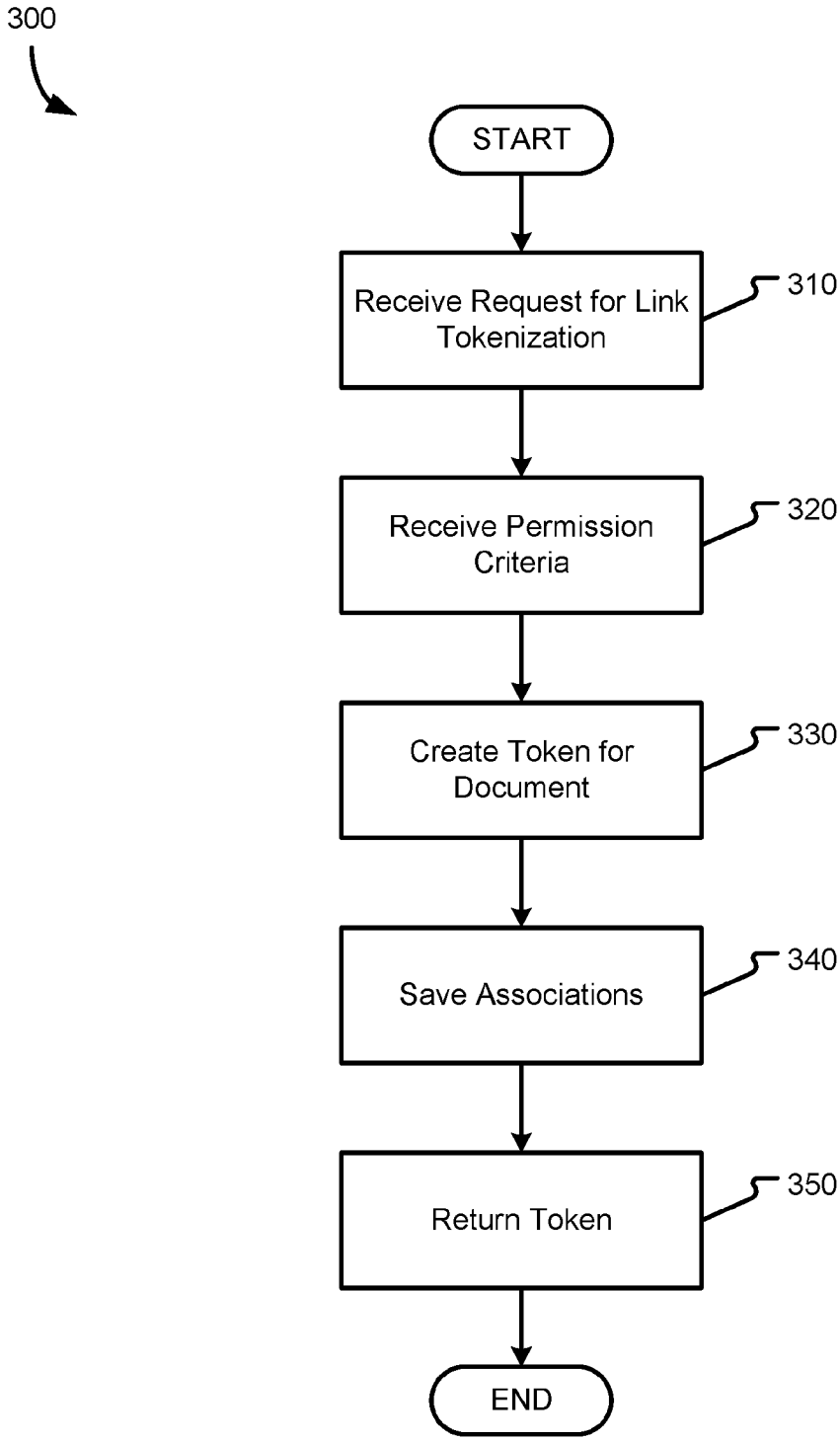

300
START
Receive Request for Link Tokenization
310
Receive Permission Criteria
320
Create Token for Document
330
Save Associations
340
Return Token
350
END

FIG. 3

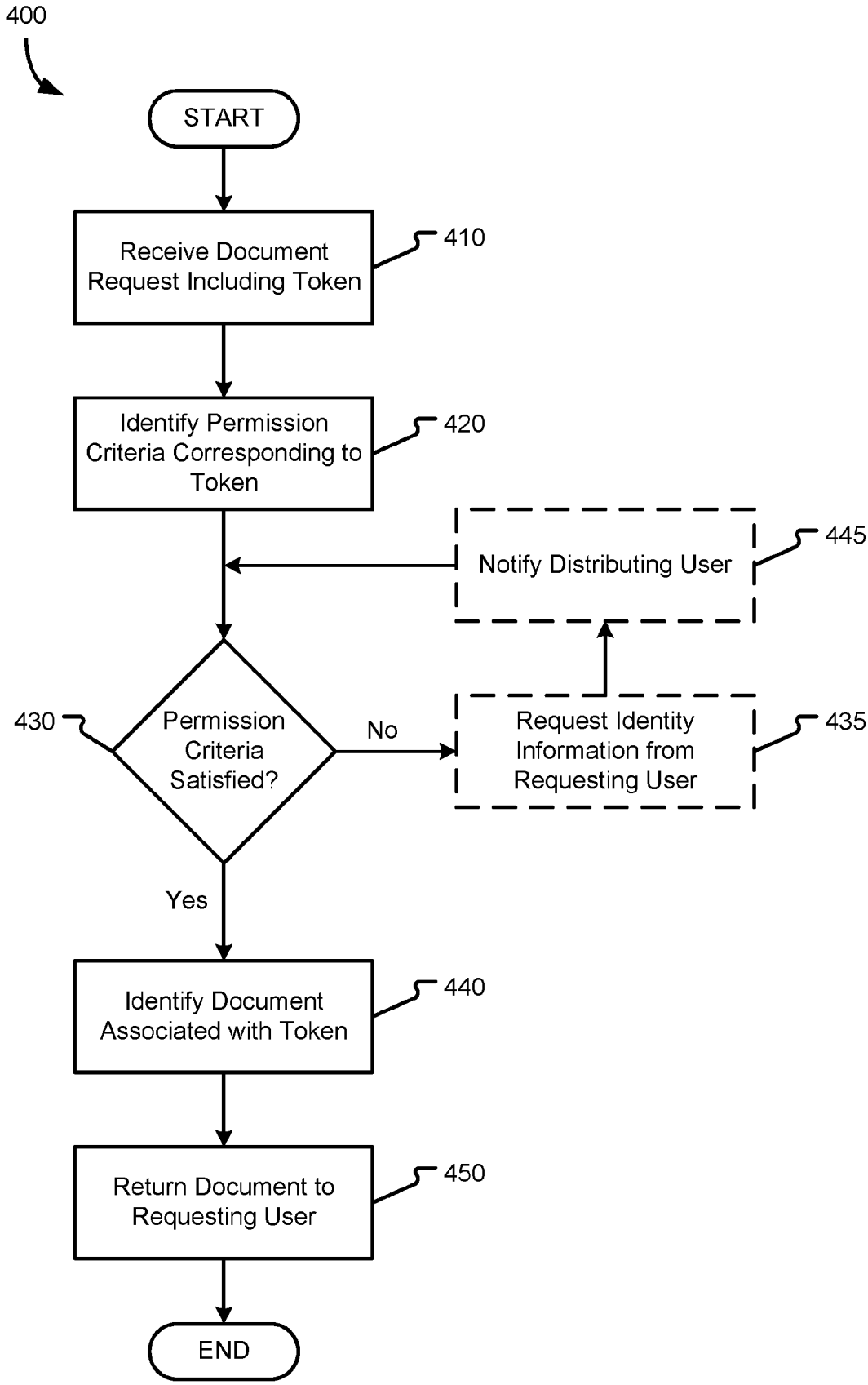

400
START
Receive Document Request Including Token
410
Identify Permission Criteria Corresponding to Token
420
Notify Distributing User
445
430
Permission Criteria Satisfied?
No
Request Identity Information from Requesting User
435
Yes
Identify Document Associated with Token
440
Return Document to Requesting User
450
END

FIG. 4

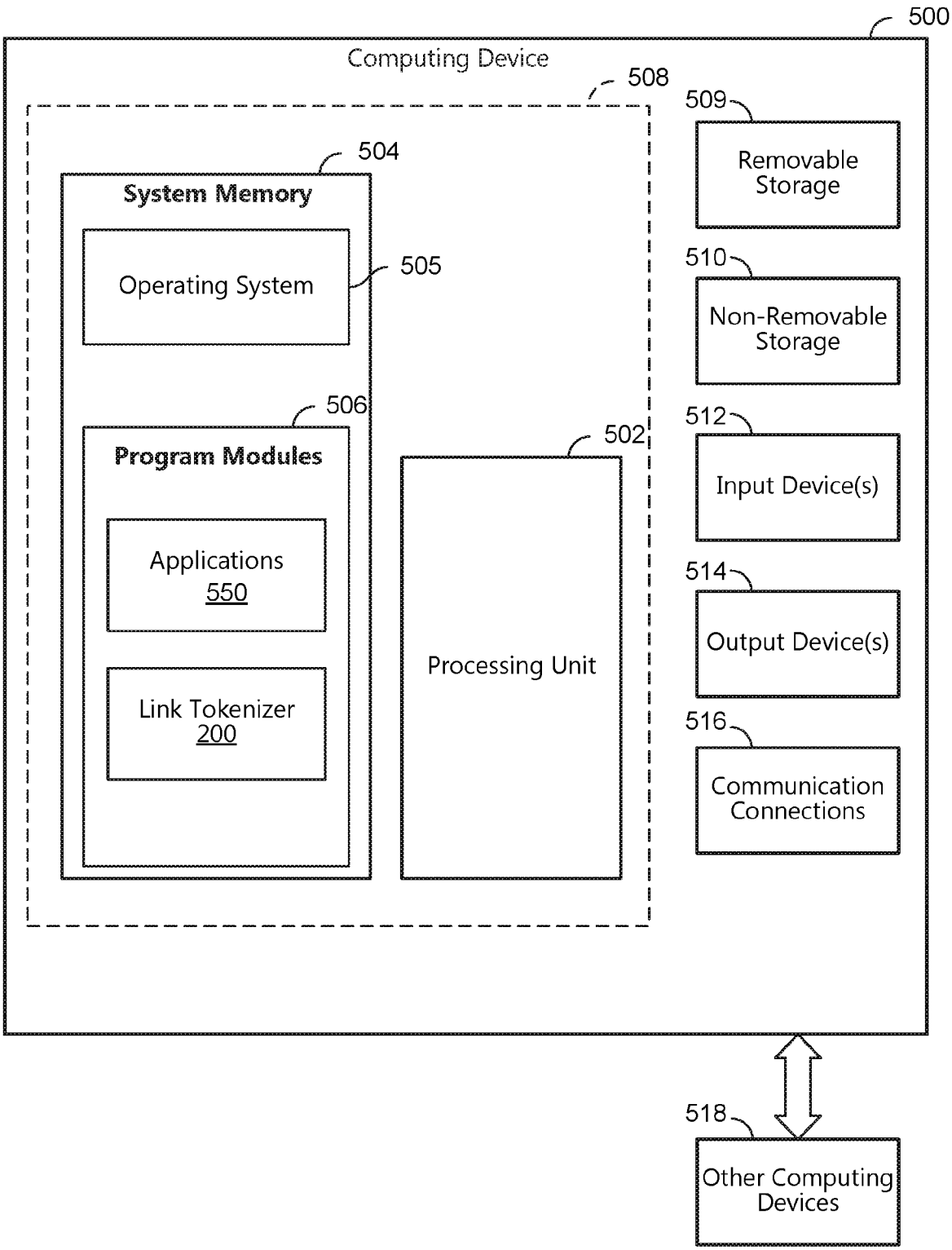
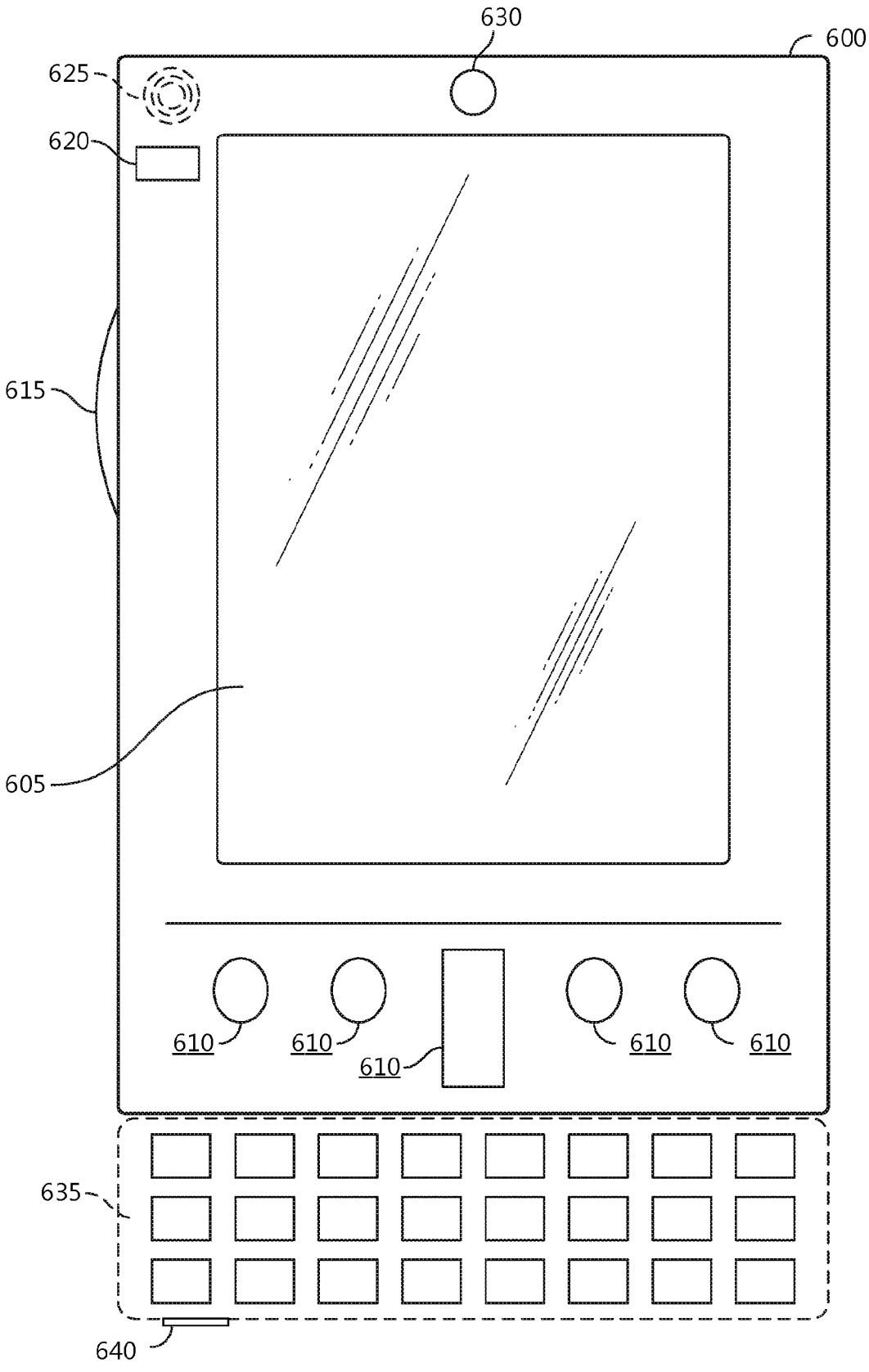

500
Computing Device
508
509
Removable Storage
504
System Memory
Operating System
505
510
Non-Removable Storage
506
Program Modules
Applications 550
Link Tokenizer 200
502
Processing Unit
512
Input Device(s)
514
Output Device(s)
516
Communication Connections
518
Other Computing Devices

FIG. 5



MOBILE COMPUTING DEVICE

FIG. 6A

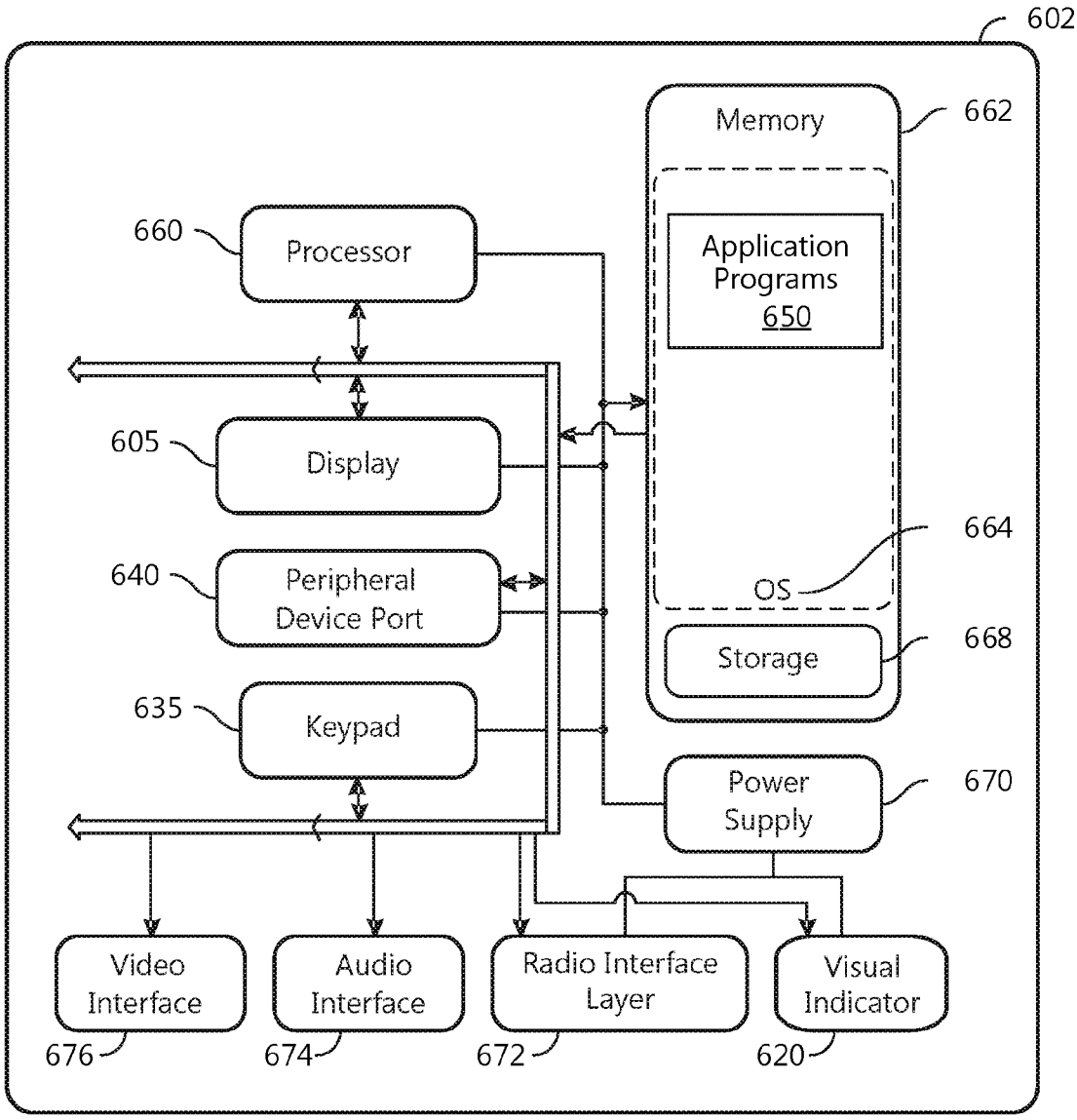

602
Memory
662
Application Programs 650
660
Processor
605
Display
640
Peripheral Device Port
664
OS
668
Storage
635
Keypad
670
Power Supply
Video Interface
676
Audio Interface
674
Radio Interface Layer
672
Visual Indicator
620

FIG. 6B

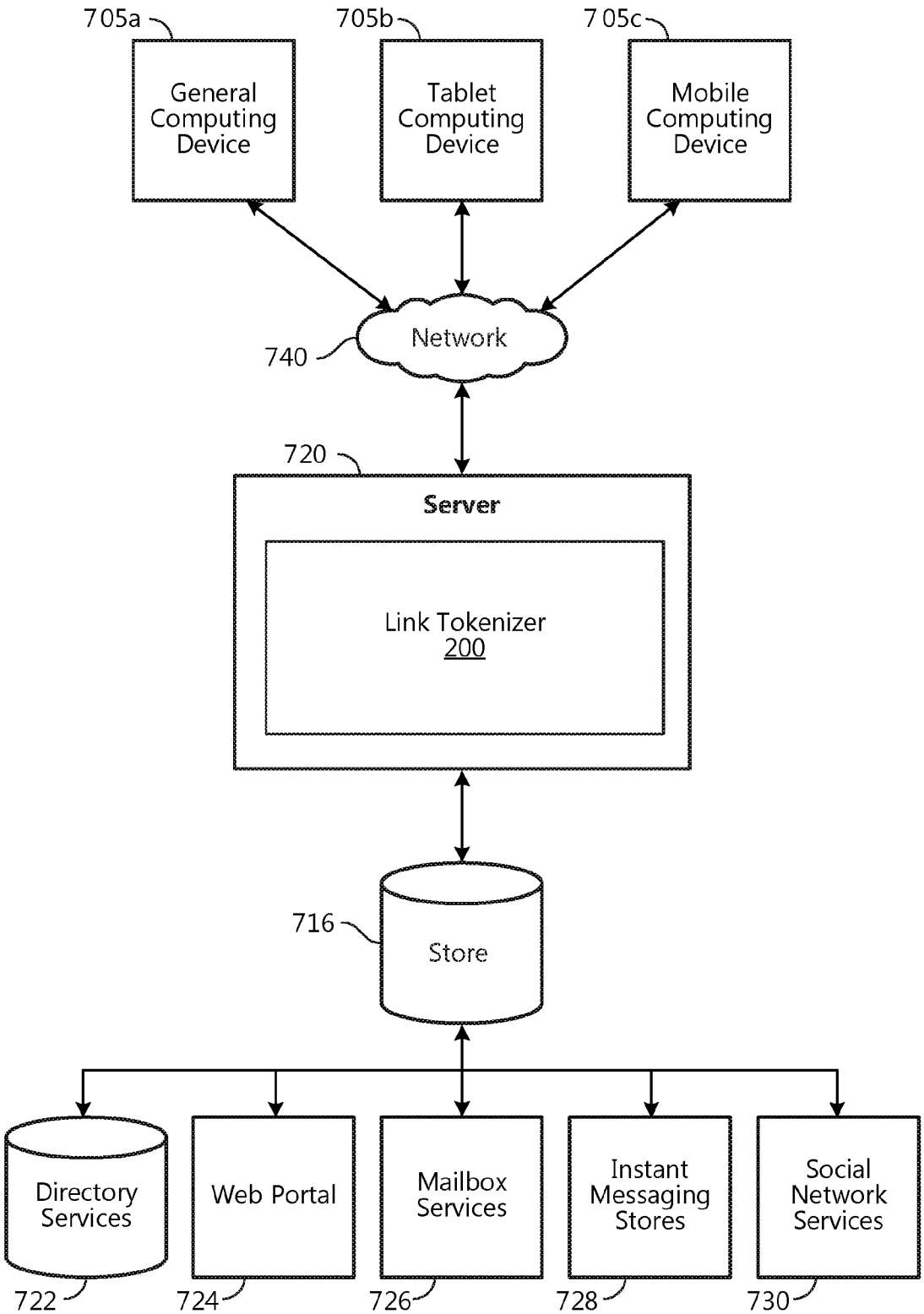

705a
General Computing Device
705b
Tablet Computing Device
705c
Mobile Computing Device
740
Network
720
Server
Link Tokenizer
200
716
Store
Directory Services
722
Web Portal
724
Mailbox Services
726
Instant Messaging Stores
728
Social Network Services
730

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/051682

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/10
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)
H04L G06F

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	US 7 272 639 B1 (LEVERGOOD THOMAS MARK [US] ET AL) 18 September 2007 (2007-09-18) column 3, lines 6-47	1-15
X	US 2003/110131 A1 (ALAIN ROSSMANN [US] ET AL) 12 June 2003 (2003-06-12) paragraphs [0013], [0089]	1-15
A	US 8 611 544 B1 (HERBACH JONATHAN [US] ET AL) 17 December 2013 (2013-12-17) column 1, line 63 - column 2, line 10 column 7, lines 37-65	1-15

☐ 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	Date of mailing of the international search report
14 November 2017	22/11/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/051682

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7272639 B1	18-09-2007	US 7272639 B1	18-09-2007
		US 8606900 B1	10-12-2013
		US 8635327 B1	21-01-2014
US 2003110131 A1	12-06-2003	DE 60218615 T2	08-11-2007
		EP 1320011 A2	18-06-2003
		JP 2003228519 A	15-08-2003
		US 7729995 B1	01-06-2010
		US 2003110131 A1	12-06-2003
		US 2008034205 A1	07-02-2008
US 8611544 B1	17-12-2013	NONE	