



- (51) International Patent Classification:
G06F 21/60 (2013.01) *G06F 21/62* (2013.01)
- (21) International Application Number:
PCT/US2017/036663
- (22) International Filing Date:
09 June 2017 (09.06.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/351,253 16 June 2016 (16.06.2016) US
15/365,847 30 November 2016 (30.11.2016) US
- (71) Applicant: MICROSOFT TECHNOLOGY LICENSING, LLC [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).
- (72) Inventors: MAYAKONTLA, Pradeep; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). OTTEWELL, Kara Lane; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). SAMNERKAR, Priya Amod; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). MUMMIDI, Lakshmi Narayana; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).
- (74) Agent: MINHAS, Sandip 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,

(54) Title: ENHANCED MANAGEMENT OF PASSWORDS FOR PRINTING APPLICATIONS AND SERVICES

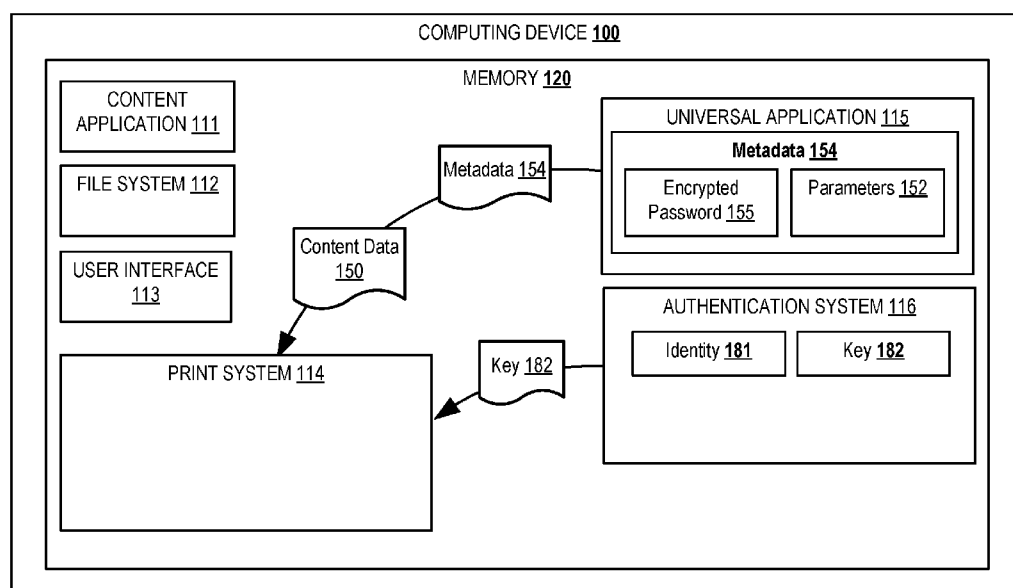


FIGURE 4

(57) **Abstract:** Techniques described herein provide enhanced management of passwords for applications and services. Generally described, the techniques disclosed herein leverage the strength of existing security measures built into operating systems to generate and communicate encrypted passwords to enable components of a computing system to operate with a heightened level of security. In some configurations, the encryption of a password using strong keys that are associated with an identity improve the security of a computing device as well as improve the security, processing, and communication of secured documents and printing schemas. In some configurations, passwords for accessing documents are encrypted and embedded in printing schemas. The encrypted password is communicated between modules of an operating system in a process for generating PDF files having improved security. The claimed techniques also leverage components of existing systems without the requirement of additional libraries.



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.

(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))*
-

ENHANCED MANAGEMENT OF PASSWORDS FOR PRINTING APPLICATIONS AND SERVICES

BACKGROUND

5 [0001] Encryption technologies provide a number of benefits to many aspects of the computing industry. For instance, encrypted files may be shared between computers while providing controlled access to the contents of the files. In one illustrative example, a user of a client computer may encrypt a file using a password. The user may share the encrypted file with a remote computer with some certainty that the contents of the file will
10 not be accessed without the password.

[0002] Although some encryption technologies provide a high level of security, one of the most common vulnerabilities of existing technologies is the communication of the password that is used to encrypt files. In some cases, when a password is communicated between software modules or components of a computing device, such communication
15 can create opportunities for password information to be lifted. Thus, even when a computer utilizes complex encryption technologies, some systems are only as secure as the techniques that are used to communicate and manage a password. The need for continual improvement in technologies for communicating and managing passwords is just as important as the need for continual development of encryption technologies.

20 [0003] It is with respect to these and other considerations that the disclosure made herein is presented.

SUMMARY

[0004] Techniques described herein provide enhanced management of passwords for applications and services. Generally described, the techniques disclosed herein leverage
25 the strength of existing security measures built into operating systems to generate and communicate encrypted passwords to enable components of a computing system to operate with a heightened level of security. In some configurations, the encryption of a password using strong keys that are associated with an identity improve the security of a computing device as well as improve the security, processing, and communication of
30 secured documents and printing schemas. In some configurations, passwords for accessing documents are encrypted and embedded in printing schemas. The encrypted password is communicated between modules of an operating system. A PDF file can then be generated by a module receiving the encrypted password. The claimed techniques leverage components of existing systems without the requirement of additional libraries.

In some configurations, encrypted data, such as an encrypted password, is generated by a universal application prior to communicating the password to a print system. Such features can increase the security of a computing device by encrypting certain types of data prior to communicating data between device components that may be vulnerable or otherwise easily compromised.

[0005] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter. The term “techniques,” for instance, may refer to system(s), method(s), computer-readable instructions, module(s), algorithms, hardware logic, and/or operation(s) as permitted by the context described above and throughout the document.

DRAWINGS

[0006] The detailed description is described with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same reference numbers in different figures indicate similar or identical items.

[0007] FIGURE 1 is a block diagram showing aspects of one example computing device disclosed herein for providing enhanced management of passwords for applications and services.

[0008] FIGURE 2 is a block diagram of the computing device shown in FIGURE 1 communicating content data.

[0009] FIGURE 3 is a block diagram of the computing device shown in FIGURE 1 communicating parameters for a portable document format, a password, and a security key.

[0010] FIGURE 4 is a block diagram of the computing device shown in FIGURE 1 communicating metadata comprising an encrypted password, content data, and a security key.

[0011] FIGURE 5 is a block diagram showing aspects of a process for generating a file having encrypted content and an encrypted password.

[0012] FIGURE 6 is a block diagram of the computing device shown in FIGURE 1 communicating a generated file to a file system, remote computer, or a printer.

[0013] FIGURE 7 illustrates a flow diagram of a routine for enabling providing enhanced management of passwords for applications and services.

[0014] FIGURE 8 is a computer architecture diagram illustrating an illustrative

computer hardware and software architecture for a computing system capable of implementing aspects of the techniques and technologies presented herein.

DETAILED DESCRIPTION

[0015] Techniques described herein provide enhanced management of passwords for applications and services. Generally described, the techniques disclosed herein leverage the strength of existing security measures built into operating systems to generate and communicate encrypted passwords to enable components of a computing system to operate with a heightened level of security. As will be described in more detail below, encryption of a password using strong keys that are associated with an identity improve the security of a computing device as well as improve the security, processing, and communication of secured documents and printing schemas. In some configurations, passwords for accessing documents are encrypted and embedded in printing schemas. Encrypted passwords are created using strong keys of an operating system and the encrypted passwords are strategically communicated between particular modules of an operating system. In some configurations, the encrypted passwords are encrypted and embedded in one or more schemas for generating PDF files having improved security. The techniques disclosed herein also leverage components of existing systems without the requirement of additional libraries.

[0016] It should be appreciated that the subject matter described herein can be implemented as a computer-controlled apparatus, a computer process, a computing system, or as an article of manufacture such as a computer-readable storage medium. These and various other features will be apparent from a reading of the following Detailed Description and a review of the associated drawings. Furthermore, the claimed subject matter is not limited to implementations that solve any or all disadvantages noted in any part of this disclosure.

[0017] As will be described in more detail herein, it can be appreciated that implementations of the techniques and technologies described herein may include the use of solid state circuits, digital logic circuits, computer component, and/or software executing on one or more devices. Signals described herein may include analog and/or digital signals for communicating a changed state, movement and/or any data associated with motion detection. Gestures, which can be in the form of any type of movement, performed by users of the computing devices can be captured by any type of sensor or input device.

[0018] While the subject matter described herein is presented in the general context of

program modules that execute in conjunction with the execution of an operating system and application programs on a computer system, those skilled in the art will recognize that other implementations may be performed in combination with other types of program modules. Generally, program modules include routines, programs, components, data
5 structures, and other types of structures that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the subject matter described herein may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, mainframe computers, and
10 the like.

[0019] By the use of the technologies described herein, enhanced management of passwords for applications and services is provided. Such technologies can improve the security of data and the security of a computing device by encrypting a password for a printing schema. Configurations disclosed herein can benefit a computing system by
15 increasing the security of a portable document format file and increasing the security of a system by reducing number of occurrences that involve the communication of an unencrypted password between components of an operating system. Other technical effects other than those mentioned herein can also be realized from implementations of the technologies disclosed herein.

[0020] In the following description, references are made to the accompanying drawings that form a part hereof, and in which are shown by way of illustration specific configurations or examples. Referring to the system drawings, in which like numerals represent like elements throughout the several figures, aspects of a computing system, computer-readable storage medium, and computer-implemented methodologies for
20 providing enhanced management of passwords for applications and services. As will be described in more detail below with respect to FIGURE 8, there are a number of applications and services that can embody the functionality and techniques described herein.

[0021] FIGURE 1 is a block diagram showing aspects of one example computing device
30 100 (also referred to herein as a “system 100”) disclosed herein for providing enhanced management of passwords for applications and services. In this illustrative example, the computing device 100 can include a local memory 120, also referred to herein as a “computer-readable storage medium,” for storing data and code modules, such as a content application 111, file system 112, user interface module 113, a print system 114, a

universal application 115, and an authentication system 116. This example is provided for illustrative purposes and is not to be construed as limiting. It can be appreciated that the computing device 100 can include any number of components, systems, and/or resources. It can also be appreciated that some of the components and data listed herein can be stored
5 and/or executed on a remote computing device in communication with the computing device 100.

[0022] In some configurations, the content application 111 can include any application suitable for processing and communicating a file. In some illustrative examples, the content application 111 can include, but is not limited to, a word processor, a spreadsheet
10 program, a browser, a presentation program, or the like. Examples of content applications 111 can include FIREFOX, CHROME, SHEETS, DOCS, etc. As will be described below, the content application 111 can generate content data by the use of one or more functions, including the execution of a print function. In one illustrative example, a “print to file” command can cause the generation of content data.

[0023] The file system 112 can include one or more modules for managing and storing files of the computing device 100. The file system 112 can include functionality for storing and managing files on a local device and/or a remote device stored on a service or remote computer. Examples of various file systems 112 can include components from an ANDROID operating system, an iOS operating system, a WINDOWS operating system,
15 to name a few.

[0024] The user interface module 113 can include one or more modules for generating a graphical user interface for display on a display device. The user interface module 113 can also include one or more modules for generating an interface that may be in the form of a generated voice using natural language technologies. The user interface module 113 can
20 also be configured to receive input data from a user using any number of suitable mechanisms including a voice input, a keyboard input, a mouse input, etc. The user interface module 113 can interpret any type of input for generating text data, such as a password and other types of input that can define fine parameters for a portable document format (PDF) file.

[0025] The print system 114 can include any type of system for processing, managing, and communicating passwords, encryption keys, content data, PDF files, and other data. In some configurations, the print system 114 can include a service, which can be referred to as a spooler. Among other operations, the print system 114 is configured to receive and process an encryption key and an encrypted password to generate a password. In addition,
30

the print system 114 is configured to utilize the password and content data to generate encrypted content data. The print system 114, as described below, is also configured to assemble different types of data, such as an encrypted password, parameter data, and encrypted content data, to generate a secured PDF file.

5 **[0026]** The universal application 115 can include one or more modules for processing and communicating passwords, encrypted passwords, parameter data, and content data. The universal application 115 can also receive, process, and communicate encryption keys. In general, the universal application 115 can be based on a platform-homogeneous application architecture, allowing the universal application 115 to run on multiple types of
10 devices. Irrespective of the underlying application architecture, the universal application 115 is configured to perform the techniques disclosed herein.

[0027] The authentication system 116 can be any suitable component of an operating system that stores, processes, and communicates encryption keys. In one illustrative example, the authentication system 116 can associate an identity 181 with an encryption
15 key 182. The authentication system 116 can verify a user by the use of one or more credentials of an identity to allow the generation, communication, and processing of one or more encryption keys 182 associated with the identity.

[0028] In some configurations, the file system 112, user interface module 113, print system 114, universal application 115, and/or the authentication system 116 are part of an
20 operating system. Examples of various operating systems having such systems and modules include, but are not limited to, the ANDROID operating system, the iOS operating system, the WINDOWS operating system, to name a few.

[0029] Referring now to FIGURES 2-6, an example data flow scenario involving the computing device 100 is shown and described. In this example, a user operating the
25 content application 111 desires to generate a password-protected PDF file. In this example, the user invokes one or more commands, such as a “print to file” or a “print to PDF” command. As shown in FIGURE 2, upon receiving a command to generate a password-protected PDF file, content data 150 is communicated from the content application 111 to the universal application 115. In one illustrative example, if the content
30 application 111 is a web browser, the content data 150 can include at least a portion of a webpage that selected for the print command.

[0030] As shown in FIGURE 3, the user interface module 113 can communicate a password 151 and one or more parameters 152 (“parameter data 152”) to the universal application 115. To facilitate such functionality, in one example, the user interface module

113 can prompt the user to enter a password 151 and one or more parameters 152 in association with the content data 150. The user interface module 113 can receive any suitable password 151 that can be used to encrypt the content data 150. The parameters 152 can include any number of aspects associated with the content data 150, such as permissions or formatting requirements desired by the user. As will be described in more detail below, when the content data 150 is embodied in a file, such as a PDF file, the parameters 152 define attributes of the file. For instance, the parameters 152 can indicate a margin size, page size, a page type, print orientation, etc. In other examples, the parameters 152 can indicate permissions for a recipient of the PDF file. For example, the permissions can permit the recipient of a PDF file containing the content data 150 to copy the contents, print the contents, modify the contents, modify comments within the file, etc. These examples are provided for illustrative purposes and are not to be construed as limiting. It can be appreciated that any type of parameter 152 can be received from a user and communicated to the universal application 115.

[0031] Also shown in FIGURE 3, an encryption key 182 is communicated from the authentication system 116 to the universal application 115. To facilitate such functionality, the authentication system 116 can store an encryption key 182 in association with an identity 181 associated with the user. The authentication system 116 can communicate the encryption key 182 to the universal application 115 when appropriate credentials associated with the identity 181 are provided by the user.

[0032] Upon receiving the password 151 and the encryption key 182, the universal application 115 utilizes the password 151 and the encryption key 182 to generate an encrypted password 155. Any suitable encryption technology can be utilized for generating the encrypted password 155. Upon generating the encrypted password 155, the universal application 115 can generate metadata 154 that includes the encrypted password 155 and the parameters 152. In some configurations, the metadata 154 is referred to in the industry as a Print Ticket schema.

[0033] As shown in FIGURE 4, upon generating the metadata 154, the universal application 115 communicates the metadata 154 and the content data 150 to the print system 114 for further processing. In addition, as shown in FIGURE 4, the encryption key 182 can also be communicated from the authentication system 116 to the print system 114.

[0034] As shown in FIGURE 5, the print system 114 utilizes the received data to obtain the password 151 and encrypt the content data 150 to generate encrypted content data 157. More specifically, the print system 114 utilizes the encryption key 182 to decrypt the

encrypted password 155 to generate the password 151. In turn, the password 151 is utilized, along with any suitable encryption technology, to encrypt the content data 150 to generate encrypted content data 157. It can be appreciated that the communication of the encrypted password 155 between the universal application 115 and the print system 114 increases the security of the system 100, as the communication of the password 151 between components can create one or more vulnerabilities.

[0035] Also shown in FIGURE 5, the print system 114 utilizes the encrypted password 155 and the encrypted content data 157 to generate a PDF file 158. In some configurations, the PDF file 158 includes the encrypted content data 157, the parameter data, and the encrypted password 155. It can be appreciated that the generated PDF file 158 can be in compliance with one or more standards, including the ISO standard. Although a PDF file 158 is utilized to illustrate aspects of the present disclosure, it can be appreciated that any suitable formatting technology can be utilized with the techniques disclosed herein.

[0036] Once the PDF file 158 is generated, as shown in FIGURE 6, the print system 114 can communicate to, and store, the PDF file 158 with any resource, such as the file system 112. It can be appreciated that the PDF file 158 can be stored on a network drive, a local drive, a remote storage service associated with an account or any other storage medium which may be on the system 100 or a remote computer (801 of FIGURE 8). In some configurations, the PDF file 158 is communicated to a printer 801.

[0037] Turning now to FIGURE 7, aspects of a routine 700 for enhanced management of passwords for applications and services are shown and described below. It should be understood that the operations of the methods disclosed herein are not necessarily presented in any particular order and that performance of some or all of the operations in an alternative order(s) is possible and is contemplated. The operations have been presented in the demonstrated order for ease of description and illustration. Operations may be added, omitted, and/or performed simultaneously, without departing from the scope of the appended claims.

[0038] It also should be understood that the illustrated methods can end at any time and need not be performed in its entirety. Some or all operations of the methods, and/or substantially equivalent operations, can be performed by execution of computer-readable instructions included on a computer-storage media, as defined below. The term “computer-readable instructions,” and variants thereof, as used in the description and claims, is used expansively herein to include routines, applications, application modules,

program modules, programs, components, data structures, algorithms, and the like. Computer-readable instructions can be implemented on various system configurations, including single-processor or multiprocessor systems, minicomputers, mainframe computers, personal computers, hand-held computing devices, microprocessor-based, programmable consumer electronics, combinations thereof, and the like.

[0039] Thus, it should be appreciated that the logical operations described herein are implemented (1) as a sequence of computer implemented acts or program modules running on a computing system and/or (2) as interconnected machine logic circuits or circuit modules within the computing system. The implementation is a matter of choice dependent on the performance and other requirements of the computing system. Accordingly, the logical operations described herein are referred to variously as states, operations, structural devices, acts, or modules. These operations, structural devices, acts, and modules may be implemented in software, in firmware, in special purpose digital logic, and any combination thereof.

[0040] For example, the operations of the routine 700 are described herein as being implemented, at least in part, by an application, component and/or circuit, such as the content application 111, file system 112, user interface module 113, a print system 114, a universal application 115, and/or the authentication system 116. In some configurations, the content application 111, file system 112, user interface module 113, a print system 114, a universal application 115, and/or the authentication system 116 can be a dynamically linked library (DLL), a statically linked library, functionality produced by an application programming interface (API), a compiled program, an interpreted program, a script or any other executable set of instructions. Data, such as the content data 150, the password 151, the metadata 154, the encrypted password 155, and the encrypted content data 157, and other data, received or processed by the content application 111, file system 112, user interface module 113, a print system 114, a universal application 115, and/or the authentication system 116 can be stored in a data structure in one or more memory components. Data can be retrieved from the data structure by addressing links or references to the data structure.

[0041] Although the following illustration refers to the components of FIGURE 1 and FIGURE 8, it can be appreciated that the operations of the routine 700 may be also implemented in many other ways. For example, the routine 700 may be implemented, at least in part, by a processor of another remote computer or a local circuit. In addition, one or more of the operations of the routine 700 may alternatively or additionally be

implemented, at least in part, by a chipset working alone or in conjunction with other software modules. Any service, circuit or application suitable for providing the techniques disclosed herein can be used in operations described herein.

5 [0042] With reference to FIGURE 7, the routine 700 begins at operation 701, where the universal application 115 receives the content data 150 from the content application 111. As summarized above, the content data 150 can include at least a portion of content that is processed by the content application 111, which can include a document, spreadsheet, webpage, or any other type of information suitable for printing and/or sharing.

10 [0043] Next, at operation 703, the universal application 115 receives an encryption key 182, a password 151 and one or more parameters 152. As summarized above, the password 151 and the parameters 152 can be obtained from one or more components receiving information from a user. The encryption key 182 can come from an authentication system 116 that stores encryption keys in association with an identity associated with the user.

15 [0044] Next, at operation 705, the universal application 115 utilizes the encryption key 182 to encrypt the password 151 thereby generating an encrypted password 155. Any number of suitable encryption technologies can be utilized for operation 705.

20 [0045] Next, at operation 707, the universal application 115 communicates the encrypted password 155 and the content data 150 to the print system 114. In addition, in some configurations, operation 707 can include the communication of the encryption key 182 from the authentication system 116 to the print system 114. In some configurations, the encrypted password 155 is embedded in a printing schema, and wherein the encrypted password 155 is embedded in the printing schema to function as salt data. In addition, by embedding an encrypted password in a printing schema, the techniques disclosed herein
25 also leverage components of existing systems without the requirement of additional libraries. This is possible because programs that read the schemas will ignore incompatible data instead of throwing errors and exceptions. However, programs configured to read the encrypted password 155 can utilize such data.

30 [0046] Next, at operation 709, the print system 114 utilizes the encryption key 182 and the encrypted password 155 to obtain the password 151. In operation 709 any suitable technology can be utilized to decrypt the encrypted password 155.

[0047] Next, at operation 711, the print system 114 utilizes the password 151 to encrypt the content data 150 to generate the encrypted content data 157. As summarized above, any suitable encryption technology can be utilized for operation 711.

[0048] Next, at operation 713, the print system 114 generates a PDF file 158 that includes the encrypted content data 157 and the encrypted password 155. As summarized above, the PDF file 158 can be configured to comply with one or more standard such as the ISO standard. Operation 713 can also involve other processes for storing and communicating the PDF file 158. For instance, the PDF file 158 can be stored in the file system 112 and/or communicated (transmitted) to a remote computing device (FIGURE 801), which may be in the form of a personal computer, a printer, a plotter, etc.

[0049] A recipient of the PDF file 158 can access the content data 150 from the PDF file 158 by the use of the password 151. In addition, a user associated with the appropriate identity can obtain the encryption key 182 and decrypt the encrypted password 155 to obtain the password 151. Such a user can then use the password 151 to decrypt the encrypted content data 157 to obtain the content data 150. Although these examples refer to the generated file as a PDF file, the generated file can also be a spool file 158. In configurations where a spool file 158 or a PDF file 158 generated and communicated to a printer or remote computer, the printer or remote computer can utilize the password 151 to print or otherwise process the contents of the spool file 158 or the PDF file 158. A spool file 158 or the PDF file 158 can also be saved to a file system.

[0050] FIGURE 8 shows additional details of an example computer architecture for the components shown in FIGURE 1 capable of executing the program components described above for providing enhanced management of passwords for applications and services. The computer architecture shown in FIGURE 8 illustrates a game console, conventional server computer, workstation, desktop computer, laptop, tablet, phablet, network appliance, personal digital assistant (“PDA”), e-reader, digital cellular phone, or other computing device, and may be utilized to execute any of the software components presented herein. For example, the computer architecture shown in FIGURE 8 may be utilized to execute any of the software components described above. Although some of the components described herein are specific to the computing devices 100, it can be appreciated that such components, and other components may be part of any suitable remote computer 801, such as the authentication system 115.

[0051] The computing device 100 includes a baseboard 802, or “motherboard,” which is a printed circuit board to which a multitude of components or devices may be connected by way of a system bus or other electrical communication paths. In one illustrative embodiment, one or more central processing units (“CPUs”) 804 operate in conjunction with a chipset 806. The CPUs 804 may be standard programmable processors that

perform arithmetic and logical operations necessary for the operation of the computing device 100.

[0052] The CPUs 804 perform operations by transitioning from one discrete, physical state to the next through the manipulation of switching elements that differentiate between and change these states. Switching elements may generally include electronic circuits that maintain one of two binary states, such as flip-flops, and electronic circuits that provide an output state based on the logical combination of the states of one or more other switching elements, such as logic gates. These basic switching elements may be combined to create more complex logic circuits, including registers, adders-subtractors, arithmetic logic units, floating-point units, and the like.

[0053] The chipset 806 provides an interface between the CPUs 804 and the remainder of the components and devices on the baseboard 802. The chipset 806 may provide an interface to a RAM 808, used as the main memory in the computing device 100. The chipset 806 may further provide an interface to a computer-readable storage medium such as a read-only memory (“ROM”) 810 or non-volatile RAM (“NVRAM”) for storing basic routines that help to startup the computing device 100 and to transfer information between the various components and devices. The ROM 810 or NVRAM may also store other software components necessary for the operation of the computing device 100 in accordance with the embodiments described herein.

[0054] The computing device 100 may operate in a networked environment using logical connections to remote computing devices and computer systems through a network, such as the local area network. The chipset 806 may include functionality for providing network connectivity through a network interface controller (NIC) 812, such as a gigabit Ethernet adapter. The NIC 812 is capable of connecting the computing device 100 to other computing devices over the network. It should be appreciated that multiple NICs 812 may be present in the computing device 100, connecting the computer to other types of networks and remote computer systems. The network allows the computing device 100 to communicate with remote services and servers, such as the remote computer 801. As can be appreciated, the remote computer 801 may host a number of services such as a printing service, a file sharing service, etc. In addition, as described above, the remote computer 801 may mirror and reflect data stored on the computing device 100 and host services that may provide data or processing for the techniques described herein.

[0055] The computing device 100 may be connected to a mass storage device 826 that provides non-volatile storage for the computing device. The mass storage device 826 may

store system programs, application programs, other program modules, and data, which have been described in greater detail herein. The mass storage device 826 may be connected to the computing device 100 through a storage controller 815 connected to the chipset 806. The mass storage device 826 may consist of one or more physical storage units. The storage controller 815 may interface with the physical storage units through a serial attached SCSI (“SAS”) interface, a serial advanced technology attachment (“SATA”) interface, a fiber channel (“FC”) interface, or other type of interface for physically connecting and transferring data between computers and physical storage units. It should also be appreciated that the mass storage device 826, other storage media and the storage controller 815 may include MultiMediaCard (MMC) components, eMMC components, Secure Digital (SD) components, PCI Express components, or the like.

[0056] The computing device 100 may store data on the mass storage device 826 by transforming the physical state of the physical storage units to reflect the information being stored. The specific transformation of physical state may depend on various factors, in different implementations of this description. Examples of such factors may include, but are not limited to, the technology used to implement the physical storage units, whether the mass storage device 826 is characterized as primary or secondary storage, and the like.

[0057] For example, the computing device 100 may store information to the mass storage device 826 by issuing instructions through the storage controller 815 to alter the magnetic characteristics of a particular location within a magnetic disk drive unit, the reflective or refractive characteristics of a particular location in an optical storage unit, or the electrical characteristics of a particular capacitor, transistor, or other discrete component in a solid-state storage unit. Other transformations of physical media are possible without departing from the scope and spirit of the present description, with the foregoing examples provided only to facilitate this description. The computing device 100 may further read information from the mass storage device 826 by detecting the physical states or characteristics of one or more particular locations within the physical storage units.

[0058] In addition to the mass storage device 826 described above, the computing device 100 may have access to other computer-readable media to store and retrieve information, such as program modules, data structures, or other data. Thus, although the content application 111, file system 112, user interface module 113, a print system 114, a universal application 115, the authentication system 116, other data and other modules are depicted

as data and software stored in the mass storage device 826, it should be appreciated that these components and/or other modules may be stored, at least in part, in other computer-readable storage media of the computing device 100. Although the description of computer-readable media contained herein refers to a mass storage device, such as a solid state drive, a hard disk or CD-ROM drive, it should be appreciated by those skilled in the art that computer-readable media can be any available computer storage media or communication media that can be accessed by the computing device 100.

[0059] Communication media includes 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 includes any delivery media. The term “modulated data signal” means a signal that has one or more of its characteristics changed or set in a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer-readable media.

[0060] By way of example, and not limitation, computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules or other data. For example, computer media includes, but is not limited to, RAM, ROM, EPROM, EEPROM, flash memory or other solid state memory technology, CD-ROM, digital versatile disks (“DVD”), HD-DVD, BLU-RAY, or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store the desired information and which can be accessed by the computing device 100. For purposes of the claims, the phrase “computer storage medium,” “computer-readable storage medium,” and variations thereof, does not include waves or signals per se and/or communication media.

[0061] The mass storage device 826 may store an operating system 827 utilized to control the operation of the computing device 100. According to one embodiment, the operating system comprises one or more components described herein. According to another embodiment, the operating system comprises the WINDOWS operating system from MICROSOFT Corporation. According to further embodiments, the operating system may comprise the UNIX, ANDROID, WINDOWS PHONE or iOS operating systems, available from their respective manufacturers. It should be appreciated that other operating systems may also be utilized. The mass storage device 826 may store other

system or application programs and data utilized by the computing devices 100, such as content application 111, file system 112, user interface module 113, a print system 114, a universal application 115, the authentication system 116, and/or any of the other software components and data described above. The mass storage device 826 might also store other programs and data not specifically identified herein.

[0062] In one embodiment, the mass storage device 826 or other computer-readable storage media is encoded with computer-executable instructions which, when loaded into the computing device 100, transform the computer from a general-purpose computing system into a special-purpose computer capable of implementing the embodiments described herein. These computer-executable instructions transform the computing device 100 by specifying how the CPUs 804 transition between states, as described above. According to one embodiment, the computing device 100 has access to computer-readable storage media storing computer-executable instructions which, when executed by the computing device 100, perform the various routines described above with regard to FIGURE 7 and the other figures. The computing device 100 might also include computer-readable storage media for performing any of the other computer-implemented operations described herein.

[0063] The computing device 100 may also include one or more input/output controllers 816 for receiving and processing input from a number of input devices, such as a keyboard, a mouse, a microphone, a headset, a touchpad, a touch screen, an electronic stylus, or any other type of input device. Also shown, the input/output controllers 816 is in communication with an input/output device 825. The input/output controller 816 may provide output to a display, such as a computer monitor, a flat-panel display, a digital projector, a printer, a plotter, or other type of output device. The input/output controller 816 may provide input communication with other devices such as a microphone 119', a speaker 119'', game controllers and/or audio devices. In addition, or alternatively, a video output 822 may be in communication with the chipset 806 and operate independent of the input/output controllers 816. It will be appreciated that the computing device 100 may not include all of the components shown in FIGURE 8, may include other components that are not explicitly shown in FIGURE 8, or may utilize an architecture completely different than that shown in FIGURE 8.

Conclusion

[0064] In closing, although the various embodiments have been described in language specific to structural features and/or methodological acts, it is to be understood that the

subject matter defined in the appended representations is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as example forms of implementing the claimed subject matter.

CLAIMS

1. A computer-implemented method, comprising:
receiving, at a universal application, content data from a content application;
receiving, at the universal application, an encryption key associated with an identity, wherein the encryption key is received from an authentication system;
receiving, at the universal application, parameter data defining aspects of a file;
receiving, at the universal application, a password;
generating, at the universal application, an encrypted password based, at least in part, on the password and the encryption key associated with the identity;
communicating the content data, the encrypted password, and the parameter data to a print system;
receiving, at the print system, the encryption key associated with the identity, wherein the encryption key is received from the authentication system;
generating, at the print system, the password from the encrypted password and the encryption key associated with the identity;
generating, at the print system, encrypted content data based, at least in part, on the password and the content data;
generating, at the print system, the file comprising the encrypted content data and the encrypted password; and
transmitting the file to a file system component or a remote computing device.
2. The method of claim 1, wherein the encrypted password is embedded in a printing schema, and wherein communicating the encrypted password to the print system comprises, communicating the printing schema from the universal application to the print system.
3. The method of claim 1, wherein the parameter data and the encrypted password are embedded in a printing schema, and wherein communicating the encrypted password and the parameter data to the print system comprises, communicating the printing schema from the universal application to the print system.
4. The method of claim 1, wherein the parameter data defines one or more formatting characteristics of the content data, and wherein the parameter data indicates one or more permissions for operations that can be performed on the content data of the file.
5. The method of claim 3, wherein the encrypted password is embedded in a printing schema, and wherein the encrypted password functions as salt data.
6. The method of claim 1, further comprising:

obtaining, at the print system, the encryption key from an operating system component based, at least in part, on credentials associated with the identity;

decrypting, at the print system, the encrypted password with the encryption key to generate the password; and

decrypting the encrypted data using the password to generate the content data.

7. A computing device, comprising:

a processor;

a memory comprising a universal application, a content application, and a print system, the memory having computer-executable instructions stored thereupon which, when executed by a computing device, cause the processor to

receive, at the universal application, content data from the content application;

receive, at the universal application, an encryption key;

receive, at the universal application, parameter data defining aspects of a portable document format file;

receive, at the universal application, a password;

generate, at the universal application, an encrypted password based, at least in part, on the password and the encryption key; and

generate schema data, wherein the schema data comprises the encrypted password and the parameter data.

8. The computing device of claim 7, wherein the computer-executable instructions further cause the processor to:

communicate the content data and the schema data, which includes the encrypted password and the parameter data, from the universal application to the print system;

receive, at the print system, the encryption key;

generate, at the print system, the password from the encrypted password and the encryption key;

generate, at the print system, encrypted content data based, at least in part, on the password and the content data; and

generate, at the print system, the portable document format file comprising the encrypted content data and the encrypted password.

9. The computing device of claim 7, wherein the encryption key is communicated from an operating system component, and wherein the encryption key is

associated with an identity at the operating system component.

10. The computing device of claim 7, wherein the parameter data defines one or more formatting characteristics of the content data.

11. The computing device of claim 7, wherein the parameter data indicates one or more permissions for operations that can be performed on the content data of the portable document format file.

12. The computing device of claim 7, wherein the encrypted password is embedded to in the schema data to function as salt data.

13. The computing device of claim 7, wherein the computer-executable instructions further cause the processor to:

obtain, at the print system, the encryption key from an operating system component based, at least in part, on credentials associated with the identity;

decrypt at the print system, the encrypted password with the encryption key to generate the password; and

decrypt the encrypted data using the password to generate the content data.

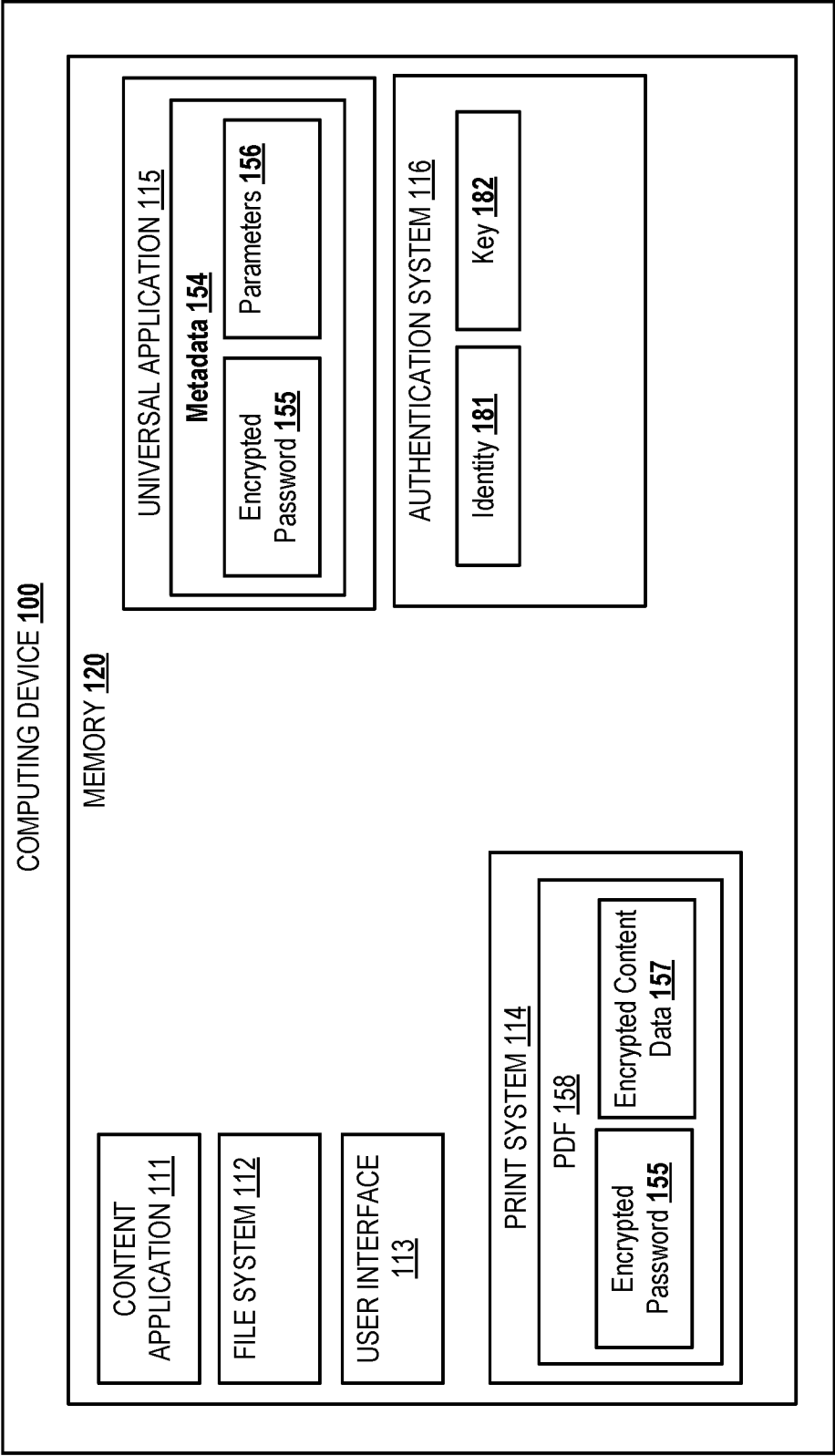


FIGURE 1

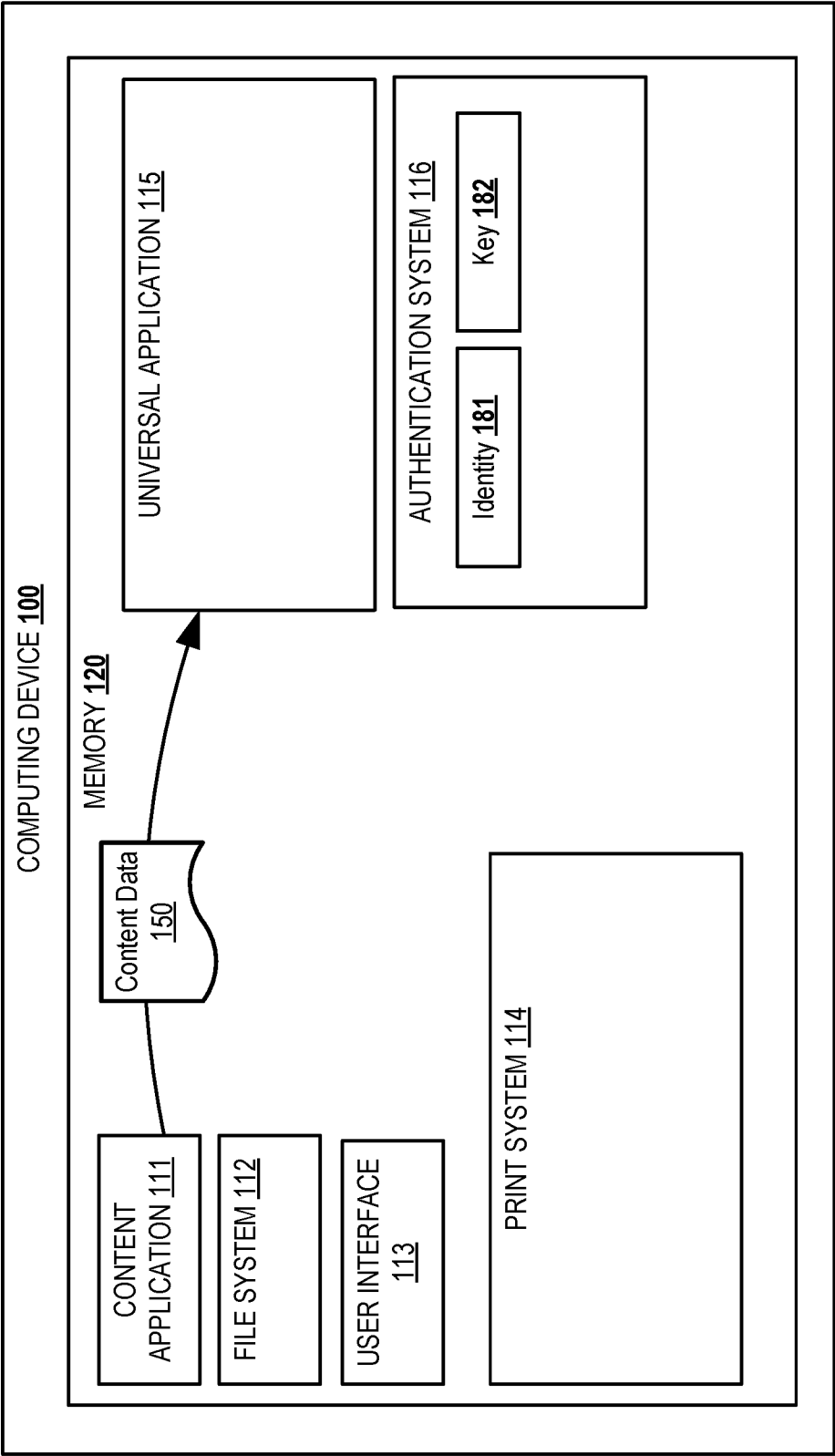


FIGURE 2

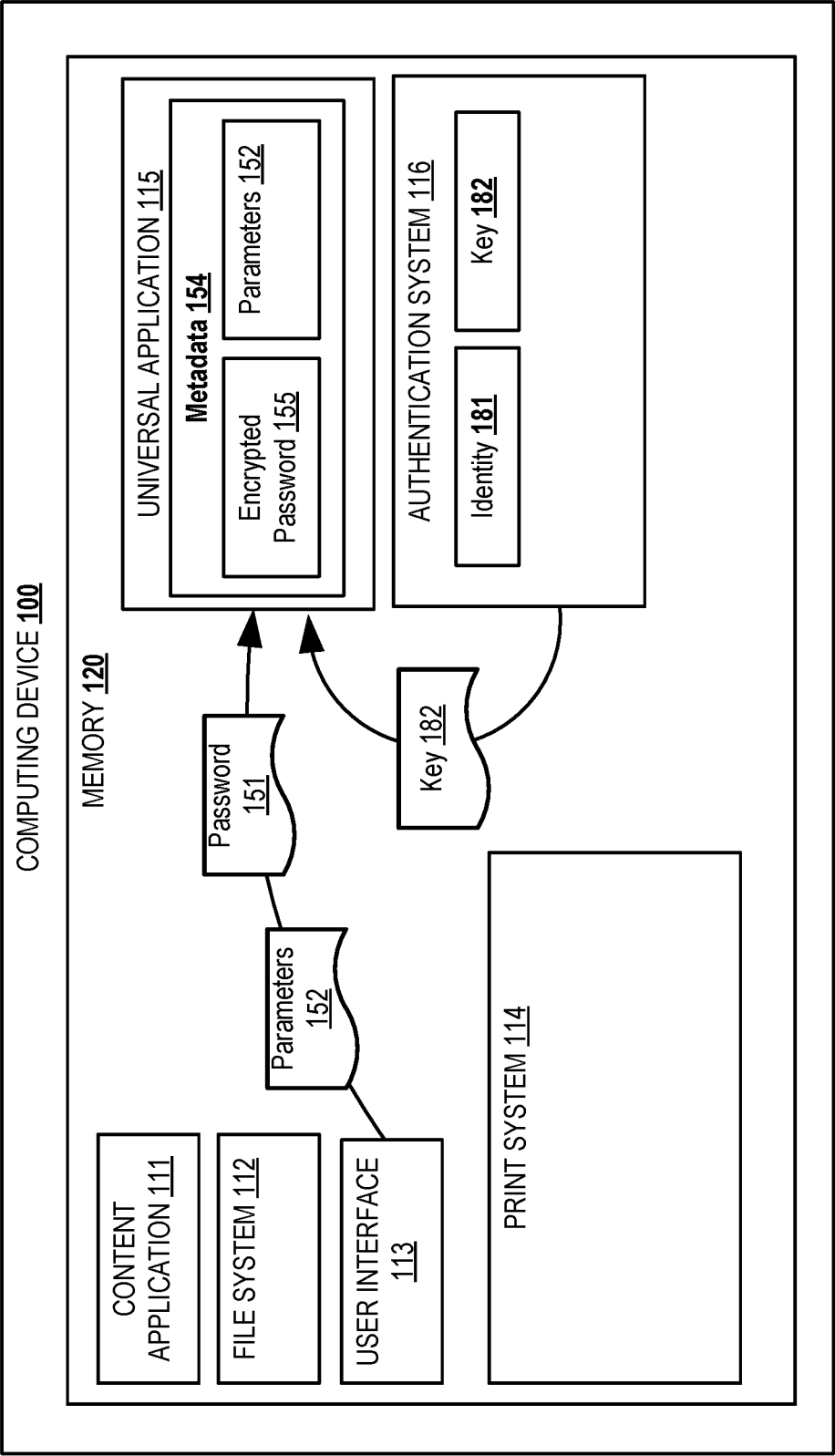


FIGURE 3

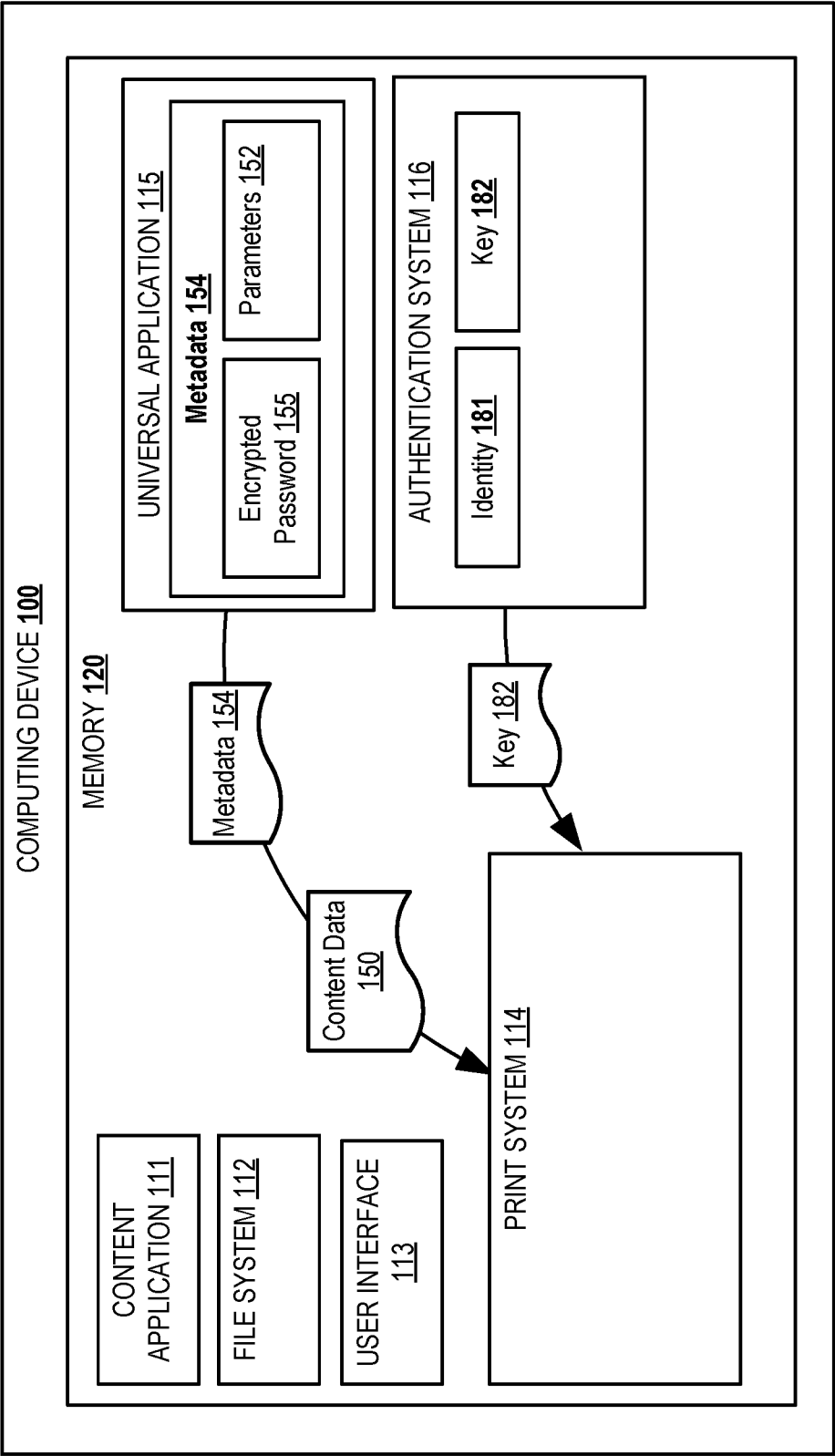


FIGURE 4

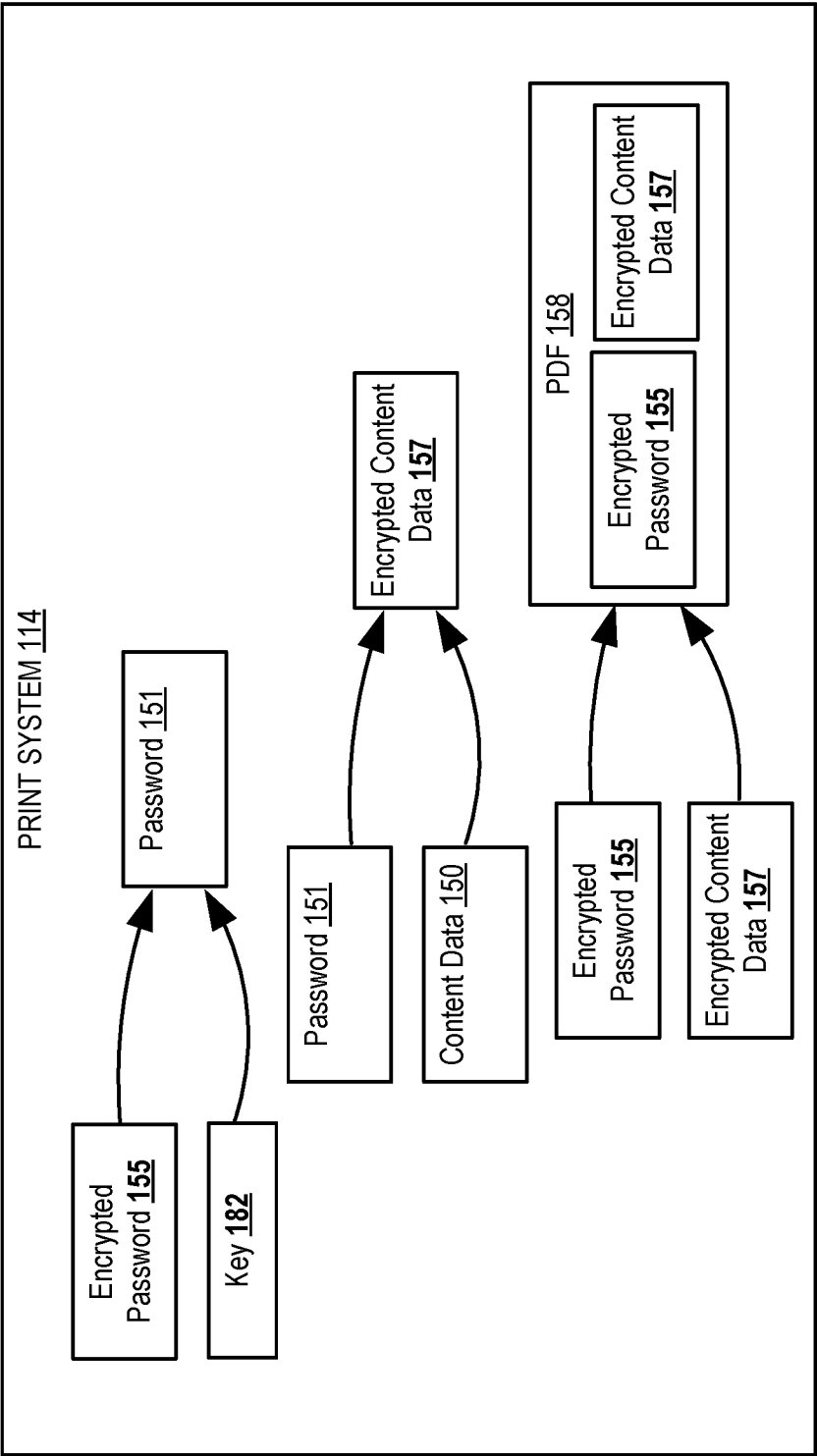


FIGURE 5

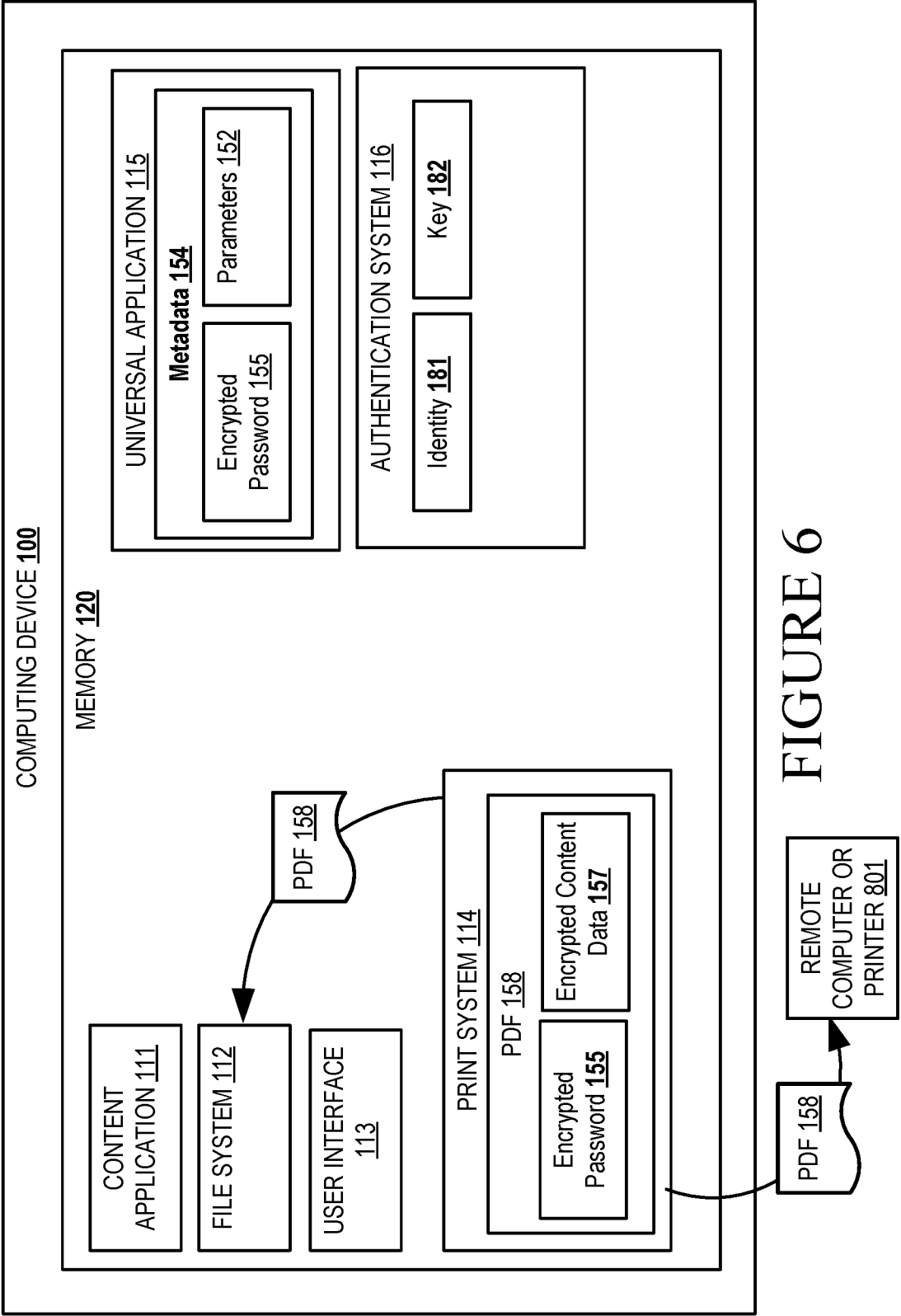


FIGURE 6

7/8

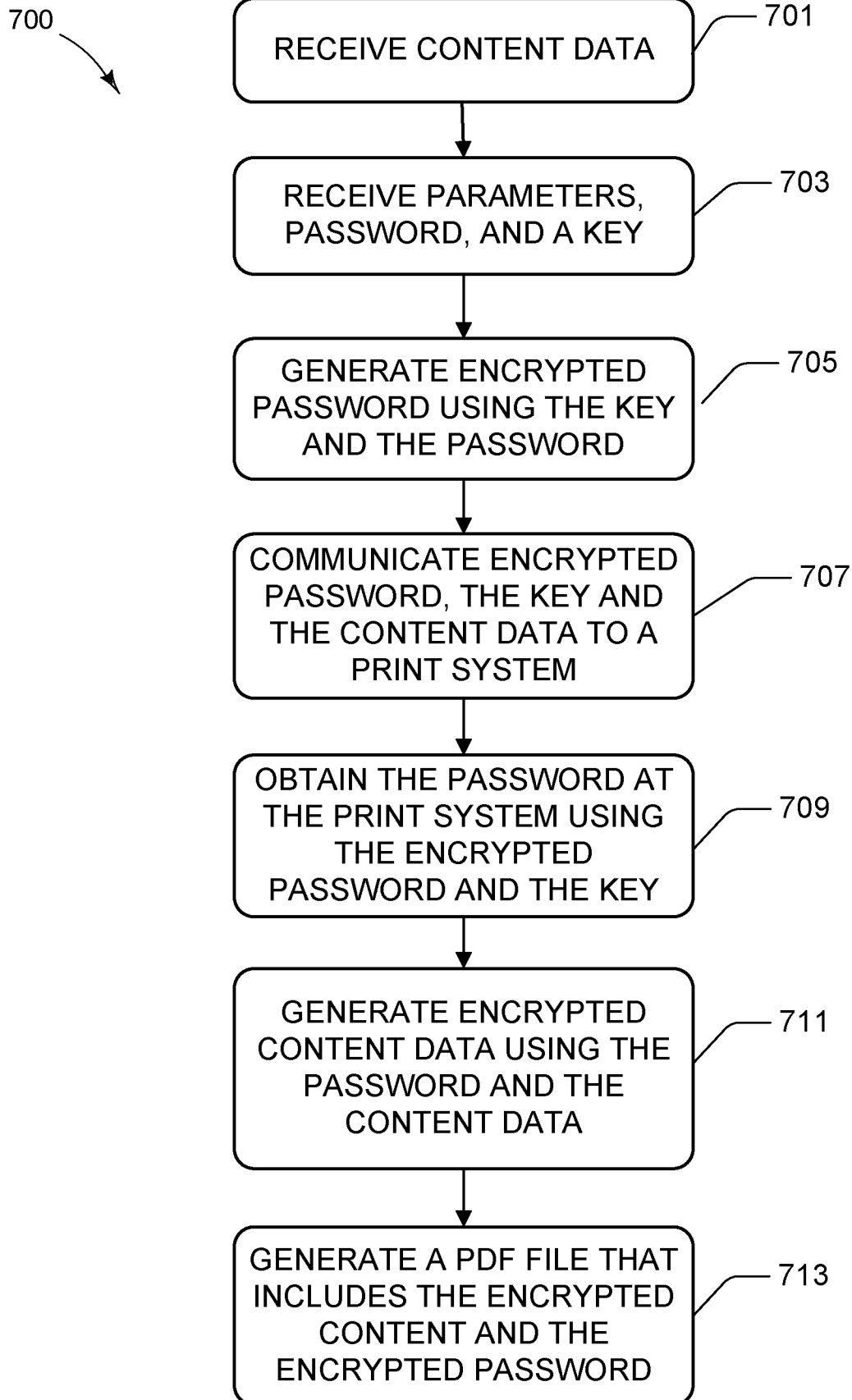


FIGURE 7

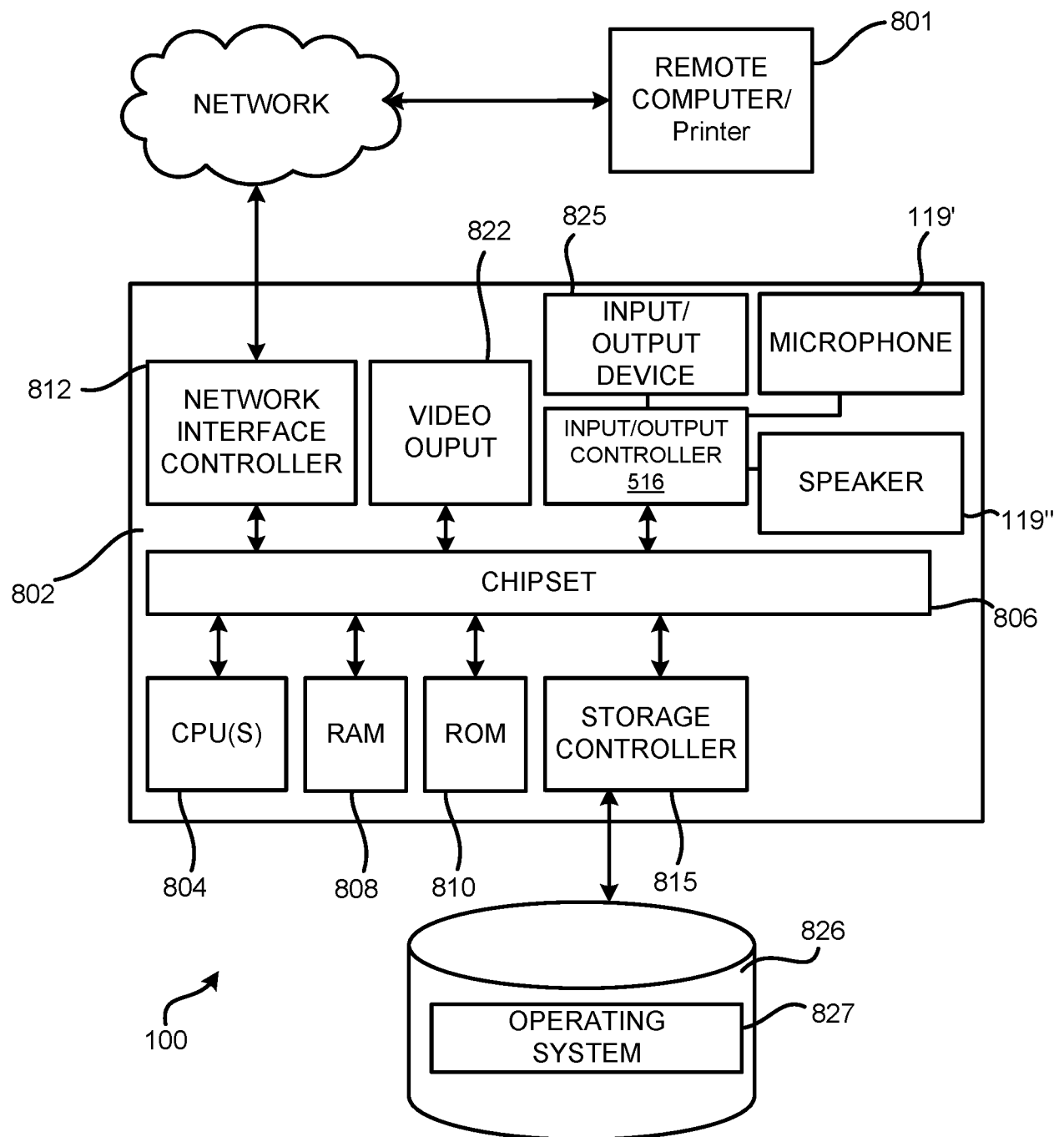


FIGURE 8

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2017/036663

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/60 G06F21/62
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)

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 2006/044589 A1 (NAKAGAWAJI SHUICHI [JP]) 2 March 2006 (2006-03-02) paragraph [0026] - paragraph [0031]; figure 1	1-13
A	----- US 6 205 549 B1 (PRAVETZ JAMES D [US]) 20 March 2001 (2001-03-20) column 2 - column 6	1-13
A	----- US 9 037 865 B1 (GOPALAKRISHNA RAJENDRA A [IN]) 19 May 2015 (2015-05-19) column 3 - column 13	1-13
A	----- US 2016/162703 A1 (KAUFMANN MICHAEL [BE]) 9 June 2016 (2016-06-09) abstract; figure 1	1-13



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

11 August 2017

Date of mailing of the international search report

22/08/2017

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

Jascou, Adrian

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/036663

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006044589	A1	02-03-2006	NONE
US 6205549	B1	20-03-2001	NONE
US 9037865	B1	19-05-2015	NONE
US 2016162703	A1	09-06-2016	CN 105474226 A 06-04-2016
			EP 3039610 A1 06-07-2016
			US 2016162703 A1 09-06-2016
			WO 2015028438 A1 05-03-2015