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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 April 2013 (04.04.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/048509 A1

(51) International Patent Classification:
G06F 3/12 (2006.01) *G06F 21/20* (2006.01)
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/US2011/054453

(22) International Filing Date:
30 September 2011 (30.09.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, M/S: RNB-4-150, Santa Clara, CA 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FALLON, Michael, F.** [US/US]; 33 Bonnieefield Drive, Tiverton, RI 02878 (US). **WILDE, Myles** [US/US]; 48 Russell Street, Charlestown, MA 02129 (US). **ADILETTA, Matthew, J.** [US/US]; 244 Sawyer Road, Bolton, MA 01740 (US).

(74) Agents: **VINCENT, Lester, J.** et al.; c/o CPA Global LLC, P.O. Box 52050, Minneapolis, MN 55402 (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) **Title**: SECURE PRINTING BETWEEN PRINTER AND PRINT CLIENT DEVICE

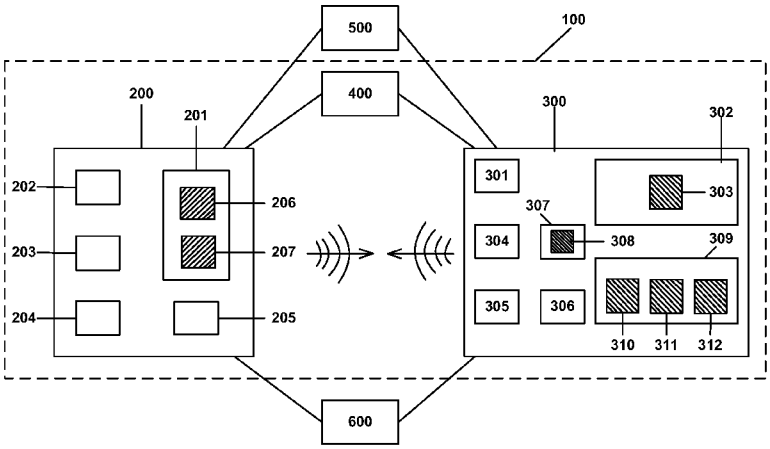

FIG. 1

(57) **Abstract**: Systems and methods of operating a computing system may involve securely printing a print document sent from a client device to a target printer. In one example, the method may include verifying an operating environment of the target printer and generating a plurality of security keys to implement asymmetric encryption of the print document.

WO 2013/048509 A1

SECURE PRINTING BETWEEN PRINTER AND PRINT CLIENT DEVICE

BACKGROUND

Technical Field

Embodiments generally relate to securely printing from a print client to a target printer. More particularly, embodiments relate to establishing a secure environment to securely print documents.

Discussion

A challenge with printing documents in public settings may be that current processes might not be secure. For example, a print request may be sent through a cloud computing infrastructure before being sent to a target printer. Printing through a cloud may be inherently insecure, as one or more computing components of the cloud may retain access to the user's document. Accordingly, a printer Original Equipment Manufacturer (OEM) may not be able to provide assurances that any document sent to a printer for printing will be handled with complete confidentiality.

BRIEF DESCRIPTION OF THE DRAWINGS

The various advantages of the embodiments of the present invention will become apparent to one skilled in the art by reading the following specification and appended claims, and by referencing the following drawings, in which:

FIG. 1 is a block diagram of an example of a computing system that utilizes a secure printing process in accordance with an embodiment of the invention; and

FIG. 2 is a flowchart of an example of a method of secure printing process in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

Embodiments may involve a computer implemented method including initializing a printer security hardware component at a target printer, verifying an integrity of an operating environment at the target printer, and receiving a request to print a document at a print client. The method may also provide for generating a plurality of security keys to implement asymmetric encryption of the document, transmitting a first security key of the plurality of security keys to the print client, and conducting an encryption of the document utilizing the first security key. The method may further provide for receiving the document at the target printer in

an encrypted form and conducting a decryption of the document utilizing a second security key of the plurality of security keys.

Embodiments can also involve a computer readable storage medium including a set of instructions, which, if executed by a processor, cause a computer to initialize a printer security hardware component at a target printer, verify an integrity of an operating environment at the target printer, and generate a plurality of security keys to implement asymmetric encryption of the document. The instructions may also cause a computer to transmit a first security key of the plurality of security keys to a print client and decrypt the document utilizing a second security key of the plurality of security keys.

In addition, embodiments may include a printer including a processing component, a security hardware component to verify an operating environment at the target printer, a memory device including a printer-side secure printing application having a set of instructions to be executed by the printer processing component, and a printer-side security logic component to decrypt the document utilizing a second security key of the plurality of security keys. If executed by a processor, the set of instructions may cause a computer to initialize the security hardware component, and generate a plurality of security keys to implement an asymmetric encryption of the document. The instructions may also cause a computer to transmit a first security key of the plurality of security keys to a print client and receive a document in an encrypted form.

Other embodiments can involve a system including a print client, a print server, and a target printer coupled to the print server. The print client may include a client transceiver, a client processing component, a client device memory having a client-side security application, and a client-side security logic component to encrypt a document. The target printer may include a printer processing component, a printer security hardware component to verify an operating environment at the target printer, a printer memory device including a printer-side secure printing application having a set of instructions to be executed by the printer processing component, and a printer-side security logic component to decrypt the document utilizing a second security key of the plurality of security keys. If executed by a processor, the instructions may cause a computer to initialize the printer security hardware component, verify an integrity of an operating environment at the target printer, and generate a plurality of security keys to implement asymmetric encryption of the document. The instructions may also cause a computer to transmit a first security key of the plurality of security keys to the print client and receive the document in an encrypted form.

Turning now to FIG. 1, a block diagram of a computing system 100 including a print client 200 and a target printer 300 is shown. The print client 200 and the target printer 300 may utilize

a secure printing process to print a document (hereinafter "document" or "print document") originating from the print client 200. The computer system 100 may also include a print server 400, and may be coupled to a cloud service 500, and a network such as the Internet 600.

The print client 200 may be any electronic device capable of issuing a print request, including a mobile device (e.g., a mobile/smart phone, a personal digital assistant, a tablet device), a notebook computer, or a desktop computer. In the embodiment illustrated in FIG. 1, the print client 200 may be a notebook computer device utilizing the Windows operating system (OS). The print client 200 may include a client device memory 201, a client processing component 202, a client transceiver 203, a client secure printing logic component 204, and a client interface 205.

The client device memory 201 may include a memory device that may be used to store data. The client device memory 201 may be built into the print client 200, or may be a removable peripheral storage device (e.g. flash memory), coupled to the client device memory 201. The client device memory 201 may store software applications including computer-readable executable instructions that may be executed by a processing component. For example, the client device memory 201 may include a client-side security application 206 and a print application 207.

The client processing component 202 may include at least one computer processor that executes computer-readable executable instructions. For example, the client-processing component 202 may execute software applications such the client-side security application 206 and the print application 207.

The client transceiver 203 may be a transmitter/receiver that enables the print client 200 to wirelessly communicate with other wirelessly-capable devices (e.g., printer 300). In this embodiment, the print client 200 and the target printer 300 communicate via a Bluetooth protocol (e.g., IEEE 802.15.1-2005, Wireless Personal Area Networks). In other embodiments of the present invention, wireless communication may take place according to other wireless communication protocols (e.g., WiFi (e.g., IEEE 802.11, 1999 Edition, LAN/MAN Wireless LANS)),

In addition, the print client 200 may include a client-side security logic component 204. The client-side security logic component 204 may be one or more logic components configured to implement a secure printing process as described herein. Indeed, as will be discussed in greater detail, at least one of the client-side security logic component 204 and the client-side security application 206 may implement at least one of receiving a first key from the target printer 300, using the first key to encrypt a document, and transmitting the encrypted document to the target printer 300.

In addition, the print client 200 may include a client interface 205 to allow a user to interact with the print client 200. The client interface 205 is a notebook display screen displaying a graphical user interface (GUI).

Turning now to the target printer 300, the target printer 300 may include any device coupled to the print client 200 capable of receiving a print request and executing it. In this embodiment, the target printer 300 includes a printer transceiver 301, a printer memory 302, a printer security hardware component 304, a printer processing component 305, a printer-side security logic 306, a printer processing assembly 307, and a printer execution assembly 309.

Similar to the client transceiver 203, the printer transceiver 301 may enable the target printer 300 to communicate wirelessly via various wireless communication protocols with other devices, such as the print client 200. In this embodiment, the printer transceiver 301 may enable the target printer 300 to communicate with the print client 200 according to a Bluetooth protocol.

The printer memory 302 may be a memory device that may be used to store data. For example, the printer memory 302 may store printer-side security application 303. As will be discussed in greater detail, the printer-side security application 303 may be a software application that may be executed to implement the secure printing process described herein.

The printer security hardware component 304 may be configured to, among other things, verify the integrity of the operating environment of the target printer 300 and ensure that the target printer 300 is operating in a known and trusted state. For example, immediately upon boot-up, the printer security hardware component 304 may verify, prior to start, the basic input/output system (BIOS). When appropriate, this may be followed by a verification, prior to start, of the operating system (OS). Again, when appropriate, these may be further followed by a verification, prior to start, of any application to be run on the target printer 300. So, for example, in the case of the printer-side security application 303, the printer security hardware component 304 may verify the printer-side security application 303 has not been hacked or modified and ensure that the printer-side security application 303 is operating in a secure and trusted compute environment. In addition, the printer security hardware component 304 may also ensure that no other processes can access the print document during the execution of a printing operation, and restricts access rights to the decrypted document only to the target printer.

The printer processing component 305 may include at least one computer processor to execute computer-readable executable instructions. For example, the printer processing component 305 may be utilized to execute software applications such a printer-side security application 303.

In addition, the target printer 300 may include printer-side security logic 306. The printer-side security logic 306 may be one or more logic components configured to implement a secure printing process as described herein.

As will be discussed in greater detail, at least one of the printer-side security application 303 and the printer-side security logic 306 may utilize, among other things, asymmetric encryption to implement a secure printing process described herein. Such asymmetric encryption may include the generation of a plurality of security keys. The generation of a plurality of security keys may include, for example, randomly generating a pair of security keys (i.e., a first key and a second key).

The pair of security keys may be utilized in conjunction with an encryption specification (e.g., Advanced Encryption Standard (AES)) to encrypt and decrypt a document to be printed. For example, the first ("public") key may be made available to any print client (e.g., print client 200) requesting to print to the target printer 300, and may be utilized to encrypt the print document. On the other hand, the second ("private") key may remain at the target printer and be kept secret, and may be utilized to decrypt the print document. A print document encrypted utilizing the first key may not be decrypting without utilizing the second key.

The printer processing assembly 307 may be an electromechanical apparatus configured to render print requests. The printer execution assembly 307 may include, among other things, a graphics engine 308.

The printer execution assembly 309 may be an electromechanical apparatus configured to execute print requests. The printer execution assembly 309 may include, among other things, a printer head 310, a supporting roller 312, and a document tray 311.

The arrangement and numbering of blocks depicted in FIG. 1 is not intended to imply an order of operations to the exclusion of other possibilities. Those of skill in the art will appreciate that the foregoing systems and methods are susceptible of various modifications and alterations. For example, in the embodiment described in FIG. 1, the printer processing component 304 and the printer-side security logic 306 may be separate, coupled components of the embodiment. However, in other embodiments of the present invention, the elements illustrated in FIG.1 may be assembled differently. For example, in another embodiment, the printer-side security logic 306 may be built into the printer processing component 304.

Turning now to FIG. 2, a flowchart of an exemplary method of printing according to one embodiment of the present invention is shown. The method might be implemented as a set of logic instructions stored in a machine- or computer-readable storage medium such as random access memory (RAM), read only memory (ROM), programmable ROM (PROM), firmware, flash memory, etc., in configurable logic such as programmable logic arrays (PLAs), field

programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), in fixed-functionality logic hardware using circuit technology such as application specific integrated circuit (ASIC), complementary metal oxide semiconductor (CMOS) or transistor-transistor logic (TTL) technology, or any combination thereof. For example, computer program code to carry out operations shown in the method may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages.

In this example, a user utilizes a notebook computer operating a Windows OS, such as print client 200 (FIG. 1) already discussed, to direct a print request for a print document to a target printer, such as the target printer 300 (FIG. 1) discussed above. Both devices may communicate wirelessly via a protocol such as, for example, the Bluetooth protocol. The method begins at processing block 2000.

At processing block 2010, at boot-up of the target printer, a printer security hardware component, such as the printer security hardware component 305 (FIG. 1) may be initialized. As discussed above, the printer security hardware component may be configured to, among other things, verify the integrity of the operating environment of the target printer, and ensure that the target printer is operating in a known and trusted state. At processing block 2020, the printer security hardware component may verify the integrity of the BIOS, and the BIOS may be started. At processing block 2030, the printer security hardware component may verify the integrity of the OS, and the OS may be started. At processing block 2040, upon the opening of an application, such as print application 207 (FIG. 1), the printer security hardware may verify the integrity of the application, and the print application may be started.

At processing block 2050, a user may initiate the print request. At processing block 2060, the print application may send a print request communication to the target printer. Upon receiving the print request, at processing block 2070, the printer security hardware component 305 may ensure that no other print processes being executed at the target printer can access the print document during execution of the print request.

At processing block 2080, a printer-side security application, such as the printer-side security application 303 (FIG. 1), may randomly generate a unique security pair, including a first key and a second key. At processing block 2090, the first key may be transmitted to the print client. At processing block 2100, the print client may utilize the first key in conjunction with a client-side security logic component, such as the client-side security logic component 204 (FIG. 1), to encrypt the print document. At processing block 2110, the encrypted print document may be transmitted to the target printer.

At processing block 2120, upon receiving the encrypted print document, the target printer may store it in a printer memory, such as the printer memory 302 (FIG. 1). Since the document is stored in its encrypted form, any unauthorized attempt to access the contents of the print document during storage can be rendered fruitless. At processing block 2130, when the target printer is ready to complete the print request, the encrypted print document may be accessed from the printer memory. At processing block 2140, the print document may be decrypted utilizing the second key in conjunction with a printer-side security logic component, such as printer-side security logic component 306 (FIG. 1).

At processing block 2150, the decrypted print document may be sent to a printer processing assembly, such as printer processing assembly 308 (FIG. 1) immediately after decrypting (i.e., processing block 2140) for print rendering. At processing block 2160, the print document may be sent for printing to a printer execution assembly, such as printer execution assembly 309 (FIG. 1), immediately after print rendering (i.e., processing block 2150).

More specifically, the printer-side security logic component (decryption), the printer processing assembly (rendering), and the printer execution assembly (printing) may be hard-wired components to process continuously without interruption. This may minimize the time the document is available in a decrypted state, thereby minimizing the likelihood of improper access. Furthermore, the print document may be decrypted into a low-level print language primitive that may provide instructions to the printer execution assembly necessary to execute the print request (e.g., instructions to the printer jets, printer rollers, etc.).

At processing block 2170, the printer execution assembly may print the print document. At processing block 2180, any versions (e.g., encrypted, decrypted) of the print document may be deleted from the target printer. At processing block 2190, the process may terminate.

The sequence and numbering of processing blocks depicted in FIG. 2 is not intended to imply an order of operations to the exclusion of other possibilities. Those of skill in the art will appreciate that the foregoing systems and methods are susceptible of various modifications and alterations.

For example, in the embodiment described in FIG. 2, after the print client sends the encrypted print document to the target printer, the print document is stored in encrypted form on the printer memory before printing. However, in other embodiments, the print document may be sent to a print server, such as the printer server 400 (FIG. 1), which may then decrypt the print document, and direct the print document to an available target printer. Also, in the embodiment described in FIG. 2, the target printer randomly generates a unique security pair. However, in other embodiments, the print server may do so. In still other embodiments, the encrypted print

document may be stored at one or more cloud service devices, such as a device associated with the cloud service 500 (FIG. 1) or elsewhere on a network, such as the Internet 600 (FIG. 1).

It will be evident to persons having the benefit of this disclosure that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the embodiments described herein. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

Those skilled in the art will appreciate from the foregoing description that the broad techniques of the embodiments of the present invention can be implemented in a variety of forms. Therefore, while the embodiments of this invention have been described in connection with particular examples thereof, the true scope of the embodiments of the invention should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, specification, and following claims.

In addition, in some of the drawings, signal conductor lines are represented with lines. Some may be thicker, to indicate more constituent signal paths, have a number label, to indicate a number of constituent signal paths, and/or have arrows at one or more ends, to indicate primary information flow direction. This, however, should not be construed in a limiting manner. Rather, such added detail may be used in connection with one or more exemplary embodiments to facilitate easier understanding. Any represented signal lines, whether or not having additional information, may actually include one or more signals that may travel in multiple directions and may be implemented with any suitable type of signal scheme, e.g., digital or analog lines implemented with differential pairs, optical fiber lines, and/or single-ended lines.

Example sizes/models/values/ranges may have been given, although embodiments of the present invention are not limited to the same. As manufacturing techniques (e.g., photolithography) mature over time, it is expected that devices of smaller size could be manufactured. In addition, well known power/ground connections and other components may or may not be shown within the figures, for simplicity of illustration and discussion, and so as not to obscure certain aspects of the embodiments of the invention. Further, arrangements may be shown in processing block diagram form in order to avoid obscuring embodiments of the invention, and also in view of the fact that specifics with respect to implementation of such block diagram arrangements are highly dependent upon the platform within which the embodiment is to be implemented, i.e., such specifics should be well within purview of one skilled in the art. Where specific details are set forth in order to describe example embodiments of the invention, it should be apparent to one skilled in the art that embodiments of the invention can be practiced without, or with variation of, these specific details. The description is thus to be regarded as illustrative instead of limiting.

The term "coupled" may be used herein to refer to any type of relationship, direct or indirect, between the components in question, and may apply to electrical, mechanical, fluid, optical, electromagnetic, electromechanical or other connections. In addition, the terms "first", "second", etc. are used herein only to facilitate discussion, and carry no particular temporal or chronological significance unless otherwise indicated.

Several features and aspects of embodiments of the present invention have been illustrated and described in detail with reference to particular embodiments by way of example only, and not by way of limitation. Those of skill in the art will appreciate that alternative implementations and various modifications to the disclosed embodiments are within the scope and contemplation of the present disclosure. Therefore, it is intended that the invention be considered as limited only by the scope of the appended claims.

CLAIMS

We claim:

1. A method comprising:

initializing a printer security hardware component at a target printer;

verifying an integrity of an operating environment at the target printer;

receiving a request to print a document at the target printer;

generating a plurality of security keys to implement asymmetric encryption of the document;

transmitting a first security key of the plurality of security keys to the print client;

conducting an encryption of the document utilizing the first security key; receiving the document at the target printer in an encrypted form; and

conducting a decryption of the document utilizing a second security key of the plurality of security keys.

2. The method of claim 1, wherein verifying the integrity of the operating environment includes verifying at least one of a basic input/output system of the target printer, an operating system of the target printer, and an application on the target printer,

3. The method claim 1, including:

rendering the document utilizing a printer processing assembly of the target printer; and

printing the document utilizing a printer execution assembly of the target printer.

4. The method of claim 1, wherein the decryption of the document is conducted at one of the target printer, a print server, and a cloud service device.

5. The method of claim 1, further including storing the document to a printer memory.

6. The method of claim 5, further including deleting the document from the printer memory.

7. The method of claim 1, further including ensuring, by the printer security hardware component, that no other print processes at the target printer can access the document during execution of the print request.

8. A computer readable storage medium comprising a set of instructions, which, if executed by a processor, cause a computer to:

initialize a printer security hardware component at a target printer;

verify an integrity of an operating environment at the target printer;

generate a plurality of security keys to implement asymmetric encryption of the document;

transmit a first security key of the plurality of security keys to a print client; and

decrypt the document utilizing a second security key of the plurality of security keys.

9. The medium claim 8, wherein, if executed, the instructions cause a computer to:

render the document at a printer processing assembly of the target printer; and

printing the document at a printer execution assembly of the target printer.

10. The medium of claim 8, wherein verifying the integrity of an operating environment at the target printer includes verifying at least one of a basic input/output system of the target printer, an operating system of the target printer, and an application on the target printer,

11. The medium of claim 8, wherein, if executed, the instructions cause a computer to store the document at a printer memory.

12. The medium of claim 11, wherein, if executed, the instructions cause a computer to delete the document from the printer memory.

13. A printer comprising:

a processing component;

a security hardware component to verify an operating environment at the printer;

a memory device including a printer-side secure printing application having a set of instructions to be executed by the processing component, wherein the printer-side secure printing application is to,

initialize the security hardware component,

generate a plurality of security keys to implement an asymmetric encryption of the document,

transmit a first security key of the plurality of security keys to a print client, and

receive a document in an encrypted form; and

a printer-side security logic component to decrypt the document utilizing a second security key of the plurality of security keys.

14. The printer of claim 13, including a processing assembly having a graphics engine to render the document.

15. The printer of claim 14, including an execution assembly having a printer head, a supporting roller, and a document tray to print the document.

16. The printer of claim 15, wherein the printer security hardware component, the printer processing assembly, and the printer execution assembly are hardwired components.

17. The apparatus of claim 13, wherein verifying the operating environment at the printer includes verifying at least one of a basic input/output system of the printer, an operating system of the printer, and an application on the printer.

18. The apparatus of claim 13, wherein the memory device is to store the document.

19. The apparatus of claim 18, wherein, if executed, the instructions cause the document to be deleted from the printer memory.

20. The apparatus of claim 13, wherein the printer-side security logic component is to decrypt the document into a low-level print language primitive.

21. A system comprising:

a print client including,

a client transceiver,

a client processing component,

a client device memory having a client-side security application, and

a client-side security logic component to encrypt a document;

a print server; and

a target printer, wherein the target printer includes,

a printer processing component,

a printer security hardware component to verify an operating environment at the target printer,

a printer memory device including a printer-side secure printing application having a set of instructions to be executed by the printer processing component, wherein the printer-side secure printing application is configured to,

initialize the printer security hardware component,

verify an integrity of the operating environment at the target printer,

generate a plurality of security keys to implement asymmetric encryption of the document,

transmit a first security key of the plurality of security keys to the print client, and

receive the document in an encrypted form, and

a printer-side security logic component to decrypt the document utilizing a second security key of the plurality of security keys.

22. The system of claim 21, wherein the printer processing component includes a graphics engine to render the document.

23. The system of claim 22, wherein the target printer includes a printer execution assembly having a printer head, a supporting roller, and a document tray to print the document.

24. The system of claim 23, wherein the printer security hardware component, the printer processing assembly, and the printer execution assembly are hardwired components.

25. The system of claim 22, wherein the target printer includes a printer memory to store the document.

26. The system of claim 25, wherein, if executed, the set of instructions cause the apparatus to delete the document from the printer memory.

27. The system of claim 22, wherein the printer security hardware component is to ensure that no other print processes at the target printer can access the document during execution of the print request.

28. The system of claim 22, wherein the printer-side security logic component is to decrypt the document into a low-level print language primitive.

29. The system of claim 21, wherein the printer security hardware component is to restrict access rights to the decrypted document only to the target printer.

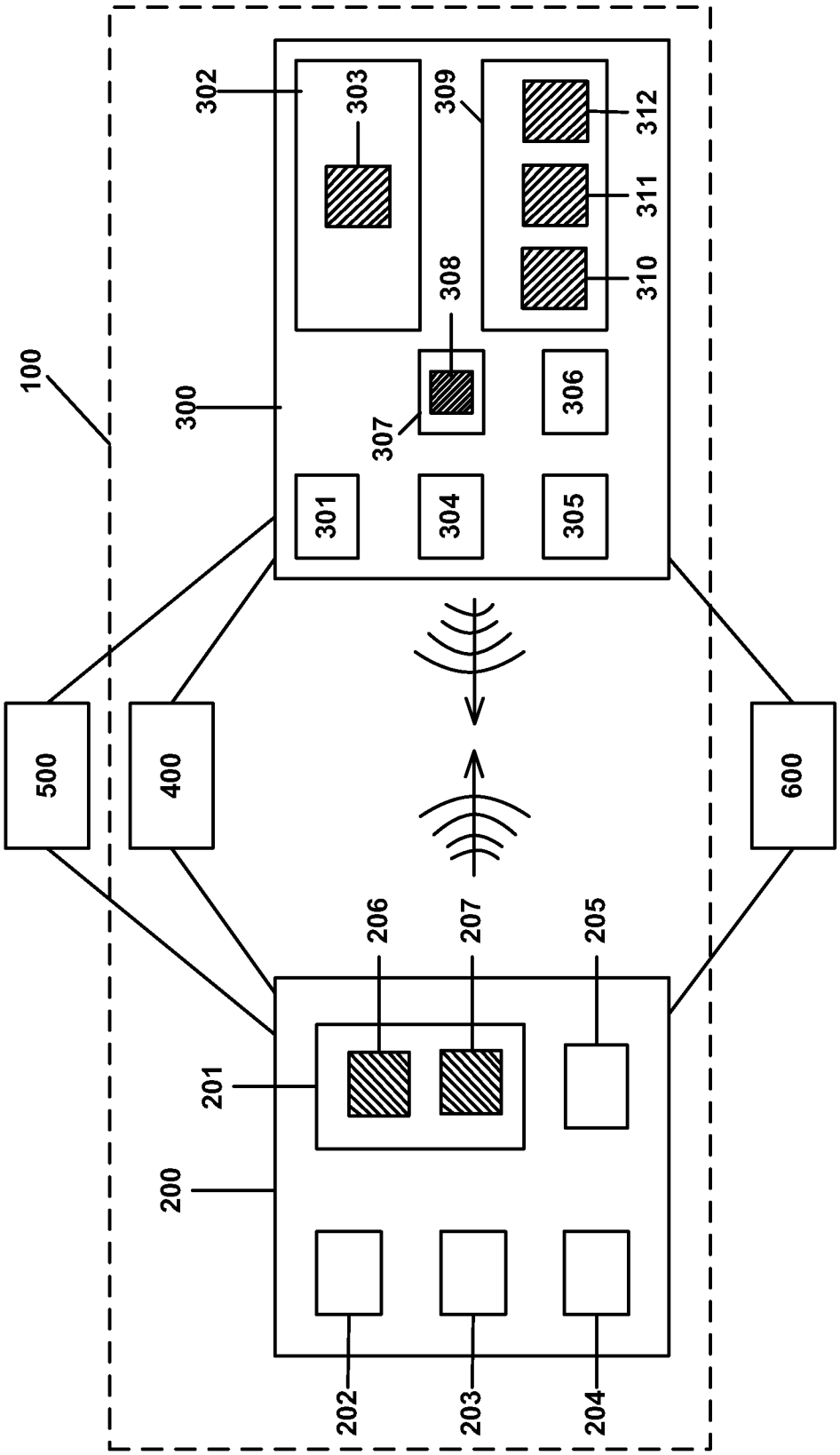
100
200
201
202
203
204
205
206
207
300
301
302
303
304
305
306
307
308
309
310
311
312
400
500
600

FIG. 1

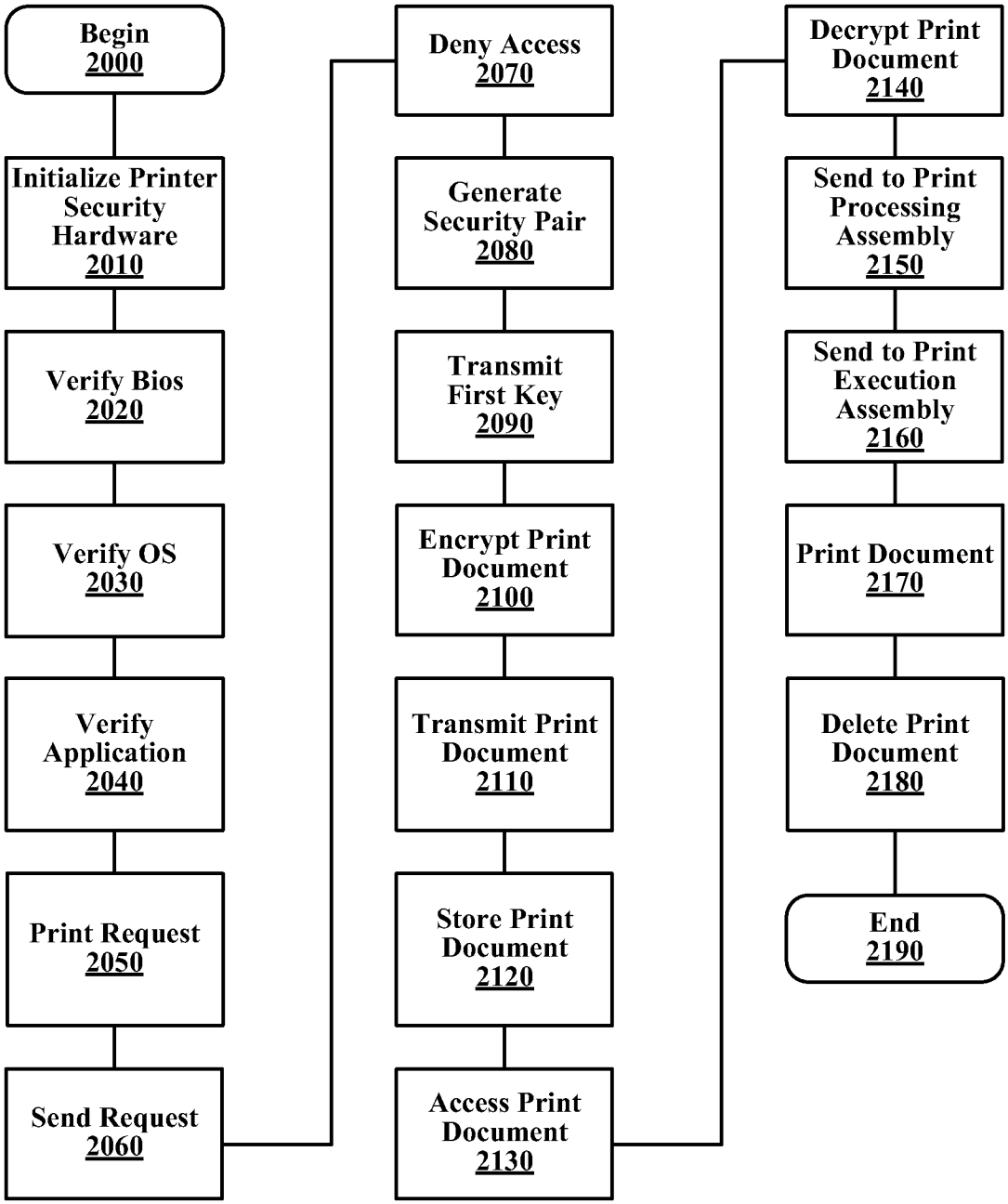
Begin
2000
Initialize Printer Security Hardware
2010
Verify Bios
2020
Verify OS
2030
Verify Application
2040
Print Request
2050
Send Request
2060
Deny Access
2070
Generate Security Pair
2080
Transmit First Key
2090
Encrypt Print Document
2100
Transmit Print Document
2110
Store Print Document
2120
Access Print Document
2130
Decrypt Print Document
2140
Send to Print Processing Assembly
2150
Send to Print Execution Assembly
2160
Print Document
2170
Delete Print Document
2180
End
2190

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/054453

A. CLASSIFICATION OF SUBJECT MATTER

G06F 3/12(2006.01)i, G06F 21/24(2006.01)i, G06F 21/20(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 3/12; H04L 9/08; G06F 15/16; G06F 17/00; G06K 15/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: printer, client, security, encrypt, decrypt, verify, integrity, asymmetric, public key, private key.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2008-097075 A (FUJI XEROX CO., LTD.) 24 April 2008 See paragraphs [0014]-[0036], [0045] and claims 1,6,16.	1-29
Y	KR 10-2011-0092516 A (TAE GIL JEONG et al.) 18 August 2011 See the abstract, paragraphs [0035]-[0037],[0045]-[0047], and claims 1-4.	1-29
Y	US 2011-0199643 A1 (BIUNDO MARC et al.) 18 August 2011 See paragraphs [0022]-[0029],[0038]-[0040] and claims 1-5.	13-29
A	US 2010-0309504 A1 (PARTRIDGE KURT E. et al.) 09 December 2010 See paragraph [0029] and claims 1-3.	1-29

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 MAY 2012 (22.05.2012)	**23 MAY 2012 (23.05.2012)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
Choi, Jae Gwi
Telephone No. 82-42-481-5787

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/054453

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2008-097075 A	24.04.2008	None	
KR 10-2011-0092516 A	18.08.2011	None	
US 2011-0199643 A1	18.08.2011	US 2004-218207 A1	04.11.2004
		US 2011-242604 A1	06.10.2011
		US 7957014 B2	07.06.2011
US 2010-0309504 A1	09.12.2010	EP 2264588 A2	22.12.2010
		EP 2264588 A3	04.01.2012
		JP 2010-282625 A	16.12.2010
		KR 10-2010-0131941 A	16.12.2010