

(51) International Patent Classification:
G06F 3/12 (2006.01)(21) International Application Number:
PCT/EP2009/061940(22) International Filing Date:
15 September 2009 (15.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08165080.6 25 September 2008 (25.09.2008) EP(71) Applicant (for all designated States except US): **OCE-TECHNOLOGIES B.V.** [NL/NL]; P.O. Box 101, St. Urbanusweg 43, NL-5914 CA Venlo (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **VAN DEN TILLAART, Robertus C.W.** [NL/NL]; Horst 77, NL-5422 BJ Genert (NL).(74) Agent: **OCE-TECHNOLOGIES B.V.**; P.O. Box 101, St. Urbanusweg 43, NL-5914 CA Venlo (NL).

(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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, SM,

[Continued on next page]

(54) Title: METHOD OF RESTRICTED PRINTING OF DOCUMENTS

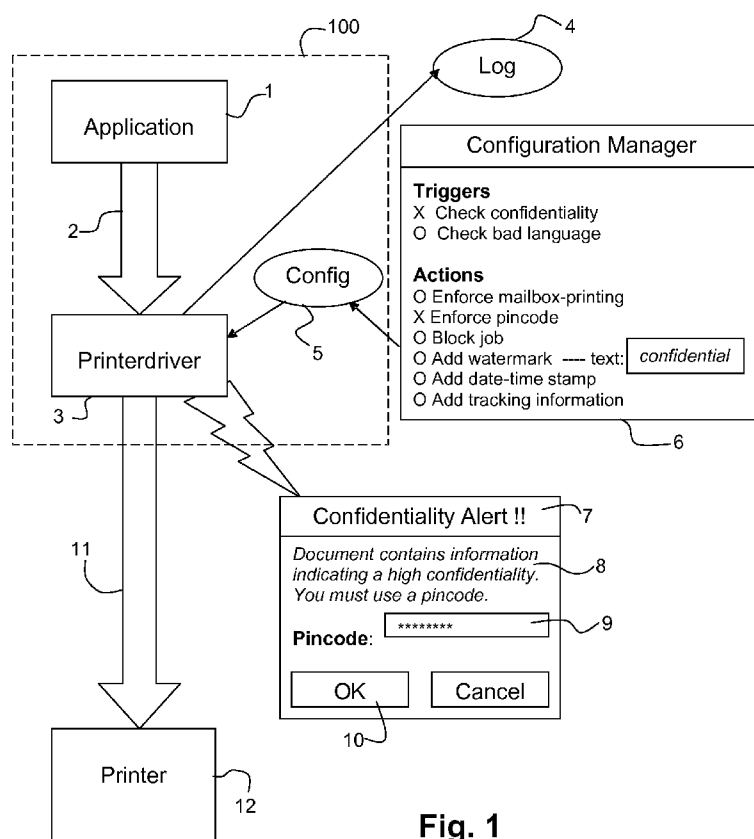


Fig. 1

(57) Abstract: The invention relates to restricted printing of documents subject to predetermined conditions. A method according to the invention comprises the steps of providing a data storage such as a database of preselected document content associated with documents of which printing is to be conditioned; sending a print command for a document to be printed to a printer driver; searching the document by the printer driver for the presence of document content contained by said database; and upon detection of such document content, subjecting printing of the document to at least one predetermined security-related action.

WO 2010/034653 A1



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
ML, MR, NE, SN, TD, TG).

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

Method of restricted printing of documents

5 The present invention relates to a method of printing documents, to a printer driver, adapted to perform said method and an associated computer program.

The present invention more specifically relates to printing documents in an environment where a printer is located in a computer network at a place where a risk is present that
10 documents printed by a first person are picked up (be it by mistake or on purpose) by a second person, or in environments where confidential documents on a computer network can be printed by persons who are not allowed to, or who may not be aware of the confidential character of the documents they print.

15 There are several ways to handle the printing of documents and at the same time preventing unwanted access to the printed documents by other people.

For instance, it is known to send print jobs for a certain printer via a computer network to a mailbox on a printer, instead of printing them directly. The mailbox then collects the
20 print jobs until it is opened on the device by a user, thereby preventing inadvertant access by people for whom the prints are not intended. Additionally, a mailbox, or individual document files, may be password protected, thus forcing the user to be present at the device before a print is made. However, it may happen that users, when submitting a print job, accidentally forget to set protection measures for their job. To
25 prevent this, all jobs may be automatically protected, but this is laborious and time-consuming, since also documents with a non-confidential character are stopped at the mailbox instead of being printed directly. It is therefore a goal of the present invention to provide a method and device that prevents the undesired or non-allowed printing of confidential documents without hampering normal operation for non-confidential print
30 jobs.

To this end, the present invention provides a method of printing documents, comprising the steps of providing a data storage, such as a database, of preselected document text content associated with documents of which printing is to be restricted; sending a print
35 command for a document to be printed to a printer driver; searching the document by

the printer driver for the presence of document text content contained by said database; and upon detection of such document text content, subjecting printing of the document to at least one predetermined security-related action.

- 5 The preselected content may be selected for a variety of reasons, among which confidentiality, appropriateness of language used, or like reasons.
The said data storage may for example be remotely located and approachable via the internet.
- 10 The mentioned predetermined security-related action may comprise warning the user, requesting user confirmation or even a plain denial to print the document, as will be described below.

Checking a print job for certain content and subjecting the printing thereof to a security-
15 related action is well-known per se, e.g. from EP-A 1 229 724, where metadata of a print job, such as the user name of the sender, are checked for permissions of that user, as contained in a database. However, the present invention does not check the metadata of a print job, but the actual text content of the document contained in the print job, that is: text content or form content of the document. In fact, the document to be printed is
20 “read” and any text content that is recognized to be the same as any of the content pre-specified in the database acts as a trigger for the security-related action.
This check is done on another level and involves different techniques than the mentioned prior art.

25 By searching a document to be printed by the printer driver, and undertaking the predetermined action related to the printing, a user who inadvertently overlooks a confidential character of the document is corrected before the document is submitted to the printer. Searching at and by the printer driver is especially advantageous, since information selected to be printed passes the printer driver before it is sent through a
30 computer network to a printer, and so the action can be undertaken before the document is sent through the network. Here, a printer driver is also to be understood as a so called pseudo printer driver, commonly used to drive faxes, generate PDF or TIFF files, or uploading documents to an archive or workflow system.

35 In an embodiment of the present invention, the preselected document content in the

data storage comprises at least one text word relating to a confidential character of the document. Those words may comprise words like "confidential", "draft", "personal", "concept", "curriculum vitae", etc. or other words that are considered to indicate confidentiality.

5

In addition, the content may be stored in the database as an expression or a rule. Such an expression may comprise a string like "\$ (space)*nnnn*", which is interpreted as an amount of money with 4 or more positions (i.e. \$ 1000 or more).

- 10 In another embodiment, the document to be printed may be based on a template that indicates a confidential character of the document. Such templates are generally characterized by certain terms at certain prescribed positions. For example an invoice or a proposal template may indicate confidentiality.
- 15 The predetermined security-related action undertaken may be of various kinds, and may for example comprise generating a user notification stating that the document is considered to be confidential. In this case, the user may decide to still print the document, or to cancel printing. Another action may be to require a confirmation from a user before the document is printed, or to force the use of a printer mailbox, also
- 20 requiring confirmation of the user at the printer. Further, the user may be requested to enter a code such as a pincode or a password, for example. The action may even be blocking the printing of the document.

- In another embodiment, the predetermined security-related action includes, that the
- 25 document is marked, with a watermark, a username, a date, a time stamp, a unique number or the like, so that it is visible for someone at the printer that this document is not intended to be read or taken by anyone different from the person who printed the document. The information the document is marked with could also serve later to trace the person who printed the document, if necessary. Especially when a username of this
- 30 person is mentioned, or the date and time when the document was printed.

- In yet another embodiment, the predetermined security-related action comprises printing the document on special paper, for example paper from a predetermined tray; or printing the document on a specific printer, for example at a specific location, where
- 35 supervision is present at the printer.

Besides confidentiality, the printer driver can further check for correctness of the document. Thereto, we propose determining the presence of hyperlinks in the document, and verifying the hyperlinks prior to printing. This way, it is avoided that documents are printed, referring to an url that does not exist anymore at the time of printing. If the url appears to be non-existent, the user may for example be prompted to provide a correct or updated url, or asked to remove the wrong url. Another option is performing a spelling and/or grammar-check on the content of the document.

10 In order to be able to perform searching the document, the searching step may include determining text content within the document, for example by performing OCR.

The present invention will now be explained referring to the following non limiting figures, in which:

- 15 - Figure 1 shows a schematic overview of the method according to the present invention; and
- Figure 2 shows a schematic overview of an internal structure of a printer driver according to the present invention.

20 Figure 1 shows a schematic overview of the method according to the present invention. In a workstation 100 of a user, an application 1 under control of the user sends a print command 2 for printing a document to a printer driver 3. The printer driver 3 keeps a log 4 of the requests for printing documents it receives and any decisions it takes in relation thereto. The log may be situated in the workstation 100 or remote, e.g. in a server (not shown).

25 Further, the printer driver 3 has a configuration file 5, which includes a list of content items associated to documents of which printing should be conditioned and a number of predetermined actions to be undertaken before printing the document. The configuration file 5 may be managed via a configuration manager 6, preferably located at a central place in the network, in which the type of action may be defined for each workstation or user, and by which for example a list of words based on which confidentiality of a document is determined, may be generated. When the printer driver 3 decides that the document for which a print request is received is confidential, it generates an alert to the user in the form of a pop-up dialog window 7 on the workstation display screen. The pop-up window 7 may comprise an explanation 8 which indicates why the document is

30

35

considered confidential, and a field 9 for entering a password or PIN code in order to enable printing of the document, after confirming the request to print the document by striking or clicking the confirmation button 10. When the user confirmation is received, the document is submitted (11) to the printer 12.

5

Here, the printer driver has a configuration file storing the content that should be filtered. This configuration file may be maintained locally on the workstation wherein print jobs are generated, but it is more efficient to install a preconfigured configuration file on a server, and to have said file distributed automatically as a part of regular software updates. In another embodiment, the printer driver may be configured to regularly connect to a server where the content that should be used for filtering is maintained centrally, and fetch the latest version of the configuration file. Also, it is possible to have a separate profile of content that should be filtered per printer driver, which is based on a name, department or role of the person who is logged on to a PC on which a print job is generated, or the network name of the PC.

Figure 2 shows a detailed view of the printer driver 3 from Figure 1. The printer driver 3 comprises a text extraction module 13 that extracts text from a print command 2 that has been received from an application 1. Once the text has been extracted, it is passed on to a language controller and comparator 14, which compares the extracted text with a list of words in the configuration file 5. If a word that indicates confidentiality is found, a pop up dialog, like the confidentiality alert window 7 in Figure 1 is generated. When a user indicates that he still desires to print the document, the document is sent (11) to the printer 12 with PIN code the user was forced to enter. When no words are found in the extracted text, that indicate confidentiality of the document, the document is directly sent to the printer.

Instead of or in addition to a pop-up dialog, various other actions are possible. For example storing a digital copy of recognized documents that are printed, or logging the printing of documents of which printing was restricted in a log file 4.

30

In another embodiment, the user may be enabled to still unrestrictedly submit the job as non-confidential, even though the document was recognized as confidential by the language controller and comparator 14. However, in that case a digital copy of the document would be stored for inspection by a supervisor.

35

Various alternative embodiments are possible, which are all comprised within the scope of the present invention, that is defined in the following claims.

CLAIMS

1. Method of restricted printing of documents,
characterized by comprising the steps of:

- 5 A. providing a data storage such as a database of preselected document text
 content associated with documents of which printing is to be restricted;
 B. sending a print command for a document to be printed to a printer driver;
 C. searching the document by the printer driver for the presence of document text
 content contained by said database; and
10 D. upon detection of such document text content, subjecting printing of the
 document to at least one predetermined security-related action.

2. Method according to claim 1, wherein the preselected document text content in the
data storage comprises at least one text word relating to a confidential character of the
15 document.

3. Method according to claim 1 or 2, wherein the preselected document text content in
the database comprises at least one document template associated with a confidential
character of the document.

20

4. Method according to any of the preceding claims, wherein the preselected document
content in the storage comprises an expression or a rule related to document text
content.

25 5. Method according to any of the preceding claims, wherein step D comprises:
 - generating a user notification stating that the document is considered to be
 confidential.

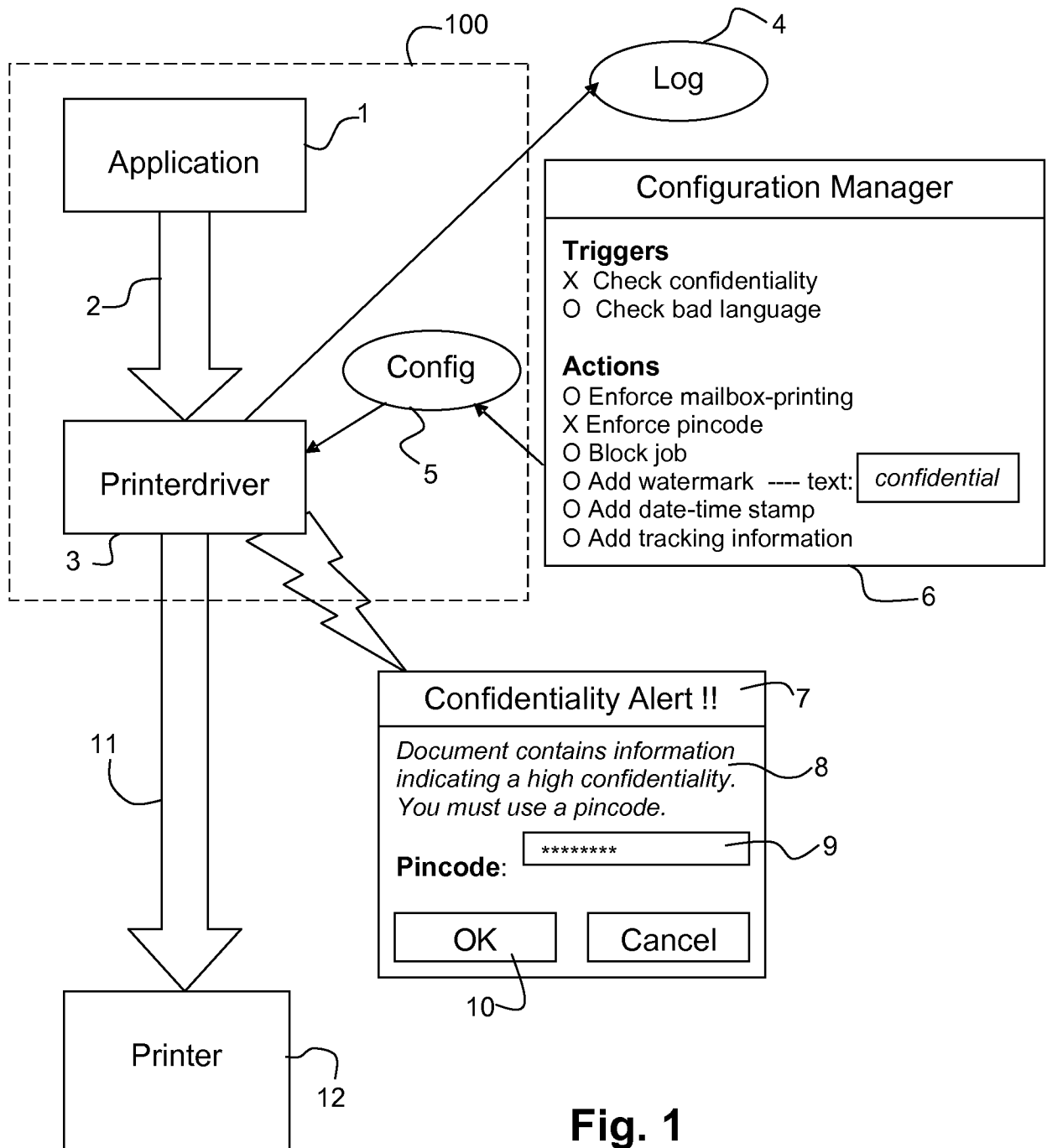
6. Method according to any of the preceding claims, wherein step D comprises:
30 - requiring a user confirmation prior to printing of the document.

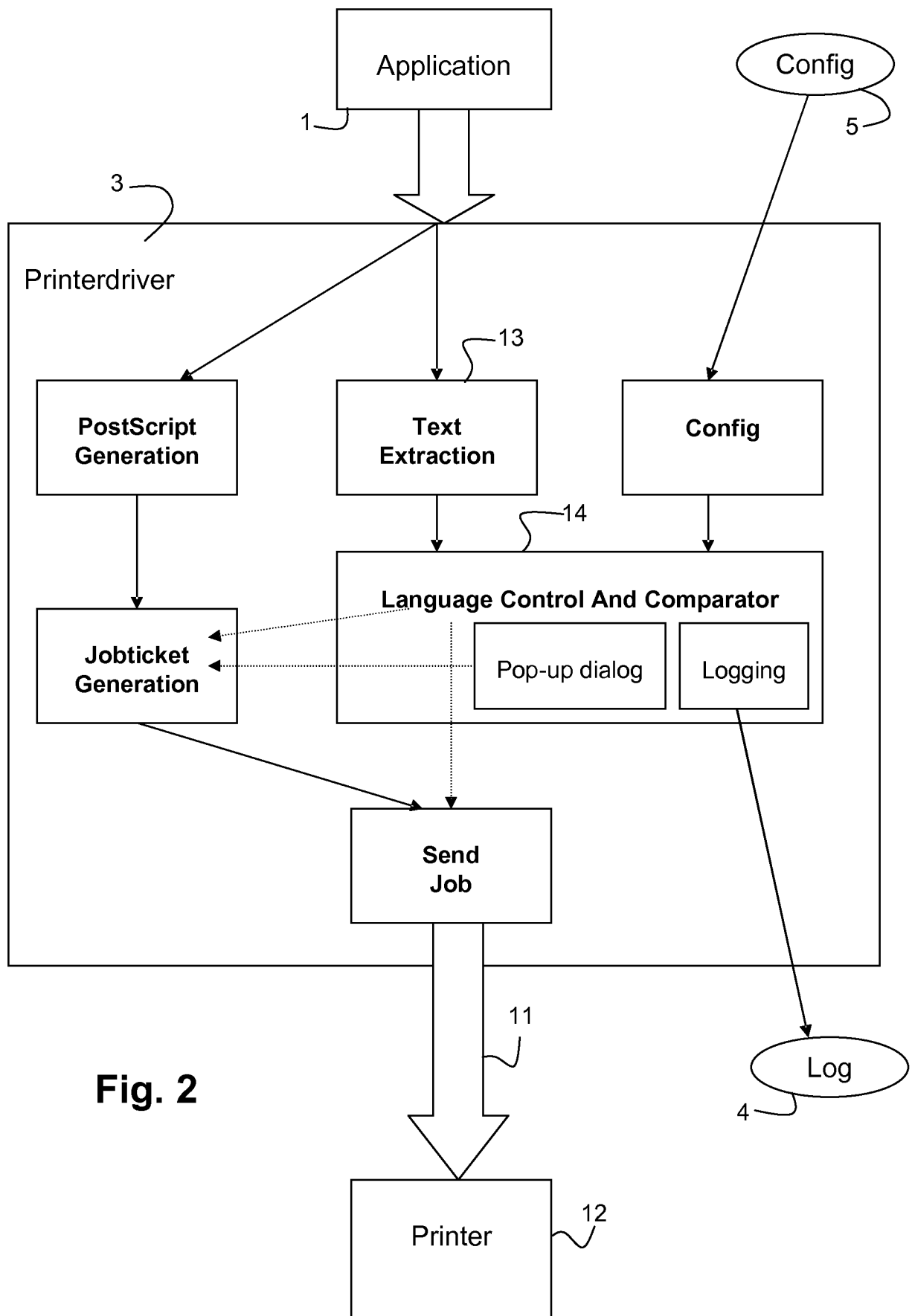
7. Method according to claim 6, wherein step D comprises:

- forcing the use of a printer mailbox, requiring user identification of the user at the
printer.

35

8. Method according to any of the preceding claims, wherein step D comprises:
- requiring a user to enter a code, to be input at the printer prior to printing of the document.
- 5 9. Method according to any of the preceding claims 1-5, wherein step D comprises:
- blocking printing of the document.
- 10 10. Method according to any of the preceding claims, wherein step D comprises marking the document, with a watermark, a username, a date, a time stamp or a unique number.
11. Method according to any of the preceding claims, wherein step D comprises:
- printing the document on paper from a predetermined paper tray of a printer; or
 - printing the document on a predetermined specific printer.
- 15 12. Method according to any of the preceding claims, wherein step C further includes determining the presence of references such as hyperlinks in the document and validating the references prior to printing of the document.
- 20 13. Method according to claim 1, wherein step C further includes performing a spelling and/or grammar-check on the content of the document.
14. Method according to any of the preceding claims, wherein step C further includes determining text content of the document, by means of OCR or a like operation.
- 25 15. Printer driver, adapted for performing a method according to any of the preceding claims.
16. Computer program comprising program code for carrying out the method of any one of claims 1 to 14, when executed on a computer.
- 30

**Fig. 1**



INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/061940

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F3/12

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 H04N

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 practical, 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	EP 1 229 724 A (OCE TECH BV [NL]) 7 August 2002 (2002-08-07) paragraph [0001] paragraph [0012] paragraph [0038] - paragraph [0040] paragraph [0045] - paragraph [0046] paragraph [0060]; figure 5 paragraph [0072] - paragraph [0076]; figure 7 paragraph [0081] - paragraph [0082]; figure 8 paragraph [0087]; figure 9 paragraph [0125] paragraph [0141]; figure 19 paragraph [0146] - paragraph [0147] paragraph [0174]; figure 24 ----- -/--	1-16



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 document 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

30 October 2009

Date of mailing of the international search report

05/11/2009

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

Limacher, Rolf

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/061940

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007 304906 A (FUJI XEROX CO LTD) 22 November 2007 (2007-11-22) abstract paragraph [0003] paragraph [0006] -----	1-16
A	JP 2004 306287 A (SHARP KK) 4 November 2004 (2004-11-04) abstract -----	11
A	JP 2008 173843 A (KONICA MINOLTA BUSINESS TECH) 31 July 2008 (2008-07-31) abstract -----	11
A	EP 1 209 897 A (XEROX CORP [US]) 29 May 2002 (2002-05-29) abstract -----	11
A	EP 1 717 742 A (OCE TECH BV [NL]) 2 November 2006 (2006-11-02) paragraph [0006] paragraph [0034] paragraph [0040] paragraph [0056] -----	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/061940

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1229724	A	07-08-2002	AU 784440 B2 06-04-2006
		AU 9516001 A	06-06-2002
		CA 2362229 A1	05-06-2002
		DE 60131242 T2	28-08-2008
		EP 1215879 A2	19-06-2002
		JP 2002199153 A	12-07-2002
		JP 3954365 B2	08-08-2007
		JP 2002236570 A	23-08-2002
JP 2007304906	A	22-11-2007	NONE
JP 2004306287	A	04-11-2004	NONE
JP 2008173843	A	31-07-2008	NONE
EP 1209897	A	29-05-2002	JP 2002190947 A 05-07-2002
EP 1717742	A	02-11-2006	NONE