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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 October 2011 (06.10.2011)

PCT

(10) International Publication Number
WO 2011/121530 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2011/051321

(22) International Filing Date:
29 March 2011 (29.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10158732.7 31 March 2010 (31.03.2010) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BAENTSCH, Michael** [DE/CH]; IBM Research GmbH, IBM Research - Zurich, Saeumerstrasse 4, CH-8803 Rueschlikon (CH). **BUHLER, Peter** [DE/CH]; IBM Research GmbH, IBM Research - Zurich, Saeumerstrasse 4, CH-8803 Rueschlikon (CH). **DYKEMAN, Harold D.** [CA/CH]; IBM Research GmbH, IBM Research - Zurich, Saeumerstrasse 4, CH-8803 Rueschlikon (CH).

(74) Agents: **RAGOT, Sébastien** et al.; IBM Research GmbH, IBM Research - Zurich, Intellectual Property Law, Säumerstrasse 4, CH-8803 Rüschlikon (CH).

(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, 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, 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,

[Continued on next page]

(54) Title: METHOD, SECURE DEVICE, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR DIGITALLY SIGNING A DOCUMENT

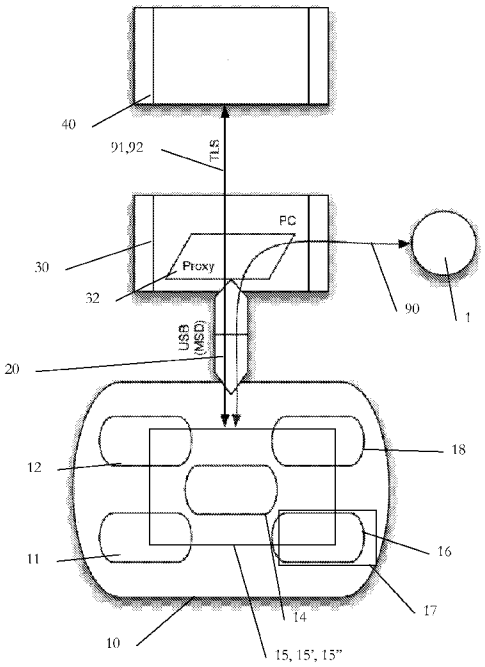


FIG. 2

(57) Abstract: The invention is notably directed to a method, a secure device and a computer program product for digitally signing a document, comprising the steps of: - providing (SI 00) a secure device (10), the secure device being protected against malicious software or malware, and adapted to establish a secure connection to a recipient (40) via a host, for example a personal computer or PC (30), connected to a telecommunication network; - after connection (S200) of the secure device to a terminal (30), accessing (S400) contents of a document received at the secure device from the terminal; - instructing (S500) at the secure device to communicate the accessed contents to an output device (12, 50) distinct from the terminal, such that said contents can be verified by a user (1); - ascertaining (S600) at the secure device a command received to digitally sign the document and executing (S700) at the secure device the ascertained command; and - instructing to send (S800) a digitally signed document to a recipient (40) over a connection (91) established via the host, the latter connected to a telecommunication network.

WO 2011/121530 A1

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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD, SECURE DEVICE, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR DIGITALLY SIGNING A DOCUMENT

FIELD OF THE INVENTION

The invention relates to a method using a secure device for digitally signing a document.

BACKGROUND OF THE INVENTION

Security problems with PCs make them unsuitable for many functions since data entered by users can be manipulated or copied by an attacker. Transactions can be changed to send money to unwanted recipients or to order unwanted goods, or user credentials can be copied providing attackers with access to systems such as those used for Internet banking.

To solve some of these problems, a user trusted device (also a "secure device") can be used together with a PC. One such solution, the IBM Zone Trusted Information Channel (see Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, Michael Baentsch, "The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks", In P. Lipp, A.-R. Sadeghi, and K.-M. Koch (Eds.): TRUST 2008, LNCS 4968, pp. 75–91, 2008), allows the user to verify information associated with a transaction (e.g., in the case of Internet banking the amount and recipient) before the transaction is executed by the service provider (e.g., the bank). The transaction is verified on the device, which is secure and can send the verified information to the back-end system in a secure manner.

Besides, secure digital document signing is one of the most significant Internet applications for the future if it can be realized efficiently and securely, given the potential to improve processes for businesses and private users (speed, security, efficiency).

A scheme based on a PC or similar device such as a smart phone is not secure since what the user sees on the device display and the document that is ultimately signed may be different. For instance, a malicious malware on the user's device can manipulate what is displayed so that it looks acceptable to the user. Thus, the document that is signed, either by the PC or a separate signature device, may be different, making any such scheme for digital signing of limited value.

It can be realized that even if the user prints the document from the device the same problem exists: a malware could alter the document sent to the printer so that it is different than the version on the device which would be signed.

Thus, a problem with existing solutions is that a user cannot trust what is shown on the display of a device that is not secure. There is accordingly a need for improving current methods for digitally signing a document.

BRIEF SUMMARY OF THE INVENTION

According to a first aspect thereof, the present invention provides a method for digitally signing a document, comprising the steps of: providing a secure device, the secure device being protected against malicious software or malware, and adapted to establish a secure connection to a recipient via a host, for example a personal computer or PC, connected to a telecommunication network; after connection of the secure device to a terminal, accessing contents of a document received at the secure device from the terminal; instructing at the secure device to communicate the accessed contents to an output device distinct from the terminal, such that said contents can be verified by a user; ascertaining at the secure device a command received to digitally sign the document and executing at the secure device the ascertained command; and instructing to send a digitally signed document to a recipient over a connection established via the host, the latter connected to a telecommunication network.

In embodiments, the method may comprise one or more of the following features:

- the method may further comprise (the terminal is the host): after connecting to the host and prior to accessing the contents of the document received, a step of instructing at the secure device to establish a connection between the secure device and a server, via the host, and receiving the document through the established connection;

- a connection established via the host is a secure connection;

- at the step of ascertaining, the received command is a command inputted by the user at the secure device; and at the step of executing the ascertained command, the command executed is a command issued by the secure device and corresponding to the command inputted by the user;

- at the step of ascertaining, the received command is a command received from or through a terminal to which the secure device is connected;

- the recipient is the server and at the step of instructing to send the digitally signed document, it is instructed to send the digitally signed document to the server, using the same connection already established with the server;

- at the step of instructing to send the digitally signed document, it is instructed to send the digitally signed document to a recipient distinct from a source of the document first received at the secure device;

- the output device is a display of the secure device and the step of instructing to communicate the contents comprises instructing to display the contents on the display of the secure device;

- the output device is an external device and the method according to the invention further comprises a step of establishing a communication between the secure device and the external device distinct from the terminal, wherein the step of instructing to communicate the contents comprises communicating the contents to the external device;

- the external device is a beamer;

- the external device is a printer;

- the step of instructing to communicate the contents comprises instructing to communicate the contents using secure Bluetooth pairing;

- the step of instructing to communicate the contents comprises instructing to communicate the contents using a USB protocol; and

- one or more secure connection established is a mutually authenticated connection such as a TLS/SSL connection.

According to another aspect, the invention is embodied as secure device having processing means, a memory and interfaces, configured to couple to or interact with: a user; a terminal such as a personal computer or PC, and a recipient, the secure device configured to establish a secure connection such as a TLS/SSL connection with a recipient via a host when the secure device is connected to the host and the latter is arranged to communicate with the recipient through a telecommunication network, and further comprising a computerized method stored on the memory and executable by the processing means for executing all the steps of the method according to the invention.

Preferably, the interfaces further comprise a display, the display adapted for displaying at least partly the said contents.

According to a further aspect, the invention is embodied as a system comprising: the secure device according to the invention, a personal computer or PC; and a server.

According to another aspect, the invention is embodied as a computer program product comprising executions executable by processing means for executing all the steps of the method according to embodiments of the invention.

Methods, devices and systems embodying the present invention will now be described, by way of non-limiting examples, and in reference to the accompanying drawings.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

- FIG. 1 is a flowchart depicting steps of a high-level embodiment of the method according to the invention;
- FIG. 2 is a schematic representation of a secure device coupled to a terminal and a server, for initiating a trustworthy connection to a server and subsequently receiving a document to be digitally signed, according to an embodiment of the invention; and
- FIG. 3 is a schematic representation of the secure device of FIG. 2, coupled to an external device, for communicating contents of a received document thereto and allowing a user to verify said contents.

DETAILED DESCRIPTION OF THE INVENTION

As an introduction to the following description, it is first pointed at a general aspect of the invention, directed to a method for digitally signing a document. The method provides a secure document management and signing operations based on a secure device (also trusted device). The secure device is protected against malicious software and configured to establish a connection (e.g., a mutually authenticated connection such as a TLS/SSL connection) to any suitable recipient/server via a terminal, e.g., a PC. This secure device can be used to securely store and manage documents received from the server or any other source. The user shall subsequently visualize the document via a display thereof or an external output device, to ensure that it is correct. The user can thus have a digital signature issued directly by the secure device (or via a terminal). Accordingly, it is possible to ensure that the document signed and sent is exactly as intended by the user.

More in details, FIG. 1 depict a flowchart illustrating an embodiment of the method. FIG. 2 is a schematic representation of a secure device coupled to a terminal and a server, for initiating a trustworthy connection to a server and subsequently receiving a document to be digitally signed, while FIG. 3 shows the secure device of FIG. 2, coupled to an external output device, for communicating contents of the document received.

Referring to FIGS. 1 – 3 altogether: first, the method uses first and foremost a secure device 10 (step S100), which is protected against malicious software or malware. In practice, the secure device has no client interfaces for software installation or other functions that would expose it to such a malware.

This device is furthermore configured to establish a connection, and preferably a secure connection such as a mutually authenticated connection, to a server and/or any suitable source or to a recipient 40, via a terminal 30. The latter is for example a PC connected to a telecommunication network such as the Internet network. In this case, a suitable type of secure connection to a server is a TLS/SSL connection. The

terminal can else be any other suitable source such as a personal digital assistant or PDA. The secure device can in all cases be suitably connected to the terminal, such as to receive a document to be processed next.

Besides, the secure device is provided with a computerized method stored on its memory for executing steps of the method described hereinafter.

Specific aspects of this device are shown in FIG. 2. Typically, the secure device 10 has processing means (or computing means) 15 coupled to a memory, which comprises both persistent and non-persistent memories 15' and 15''. The persistent memory stores e.g., the computerized method evoked above, to be executed by the said processing means.

In addition, the device is further provided with at least one interface 20, e.g., a USB interface, for communicating with the terminal, i.e. a PC 30 or any other source. In embodiments, the same interface 20 (or another type of interface) shall furthermore allow the secure device for communicating with an external device such as a beamer, a printer, or any other output device 50.

If necessary, the secure device has a card reader 17 to read user credentials stored on a memory card 16, e.g., a smart card. Suitable use can safely be made out of such data, e.g., user credentials as stored on the card. In particular, a trustworthy connection can be established between a user (or strictly speaking the device) and a third party, e.g., a server, via the terminal and using such data. In a variant, the user credentials may be stored directly on the secure device.

Further interfaces (like control buttons 18 and display 12) allow for interaction with a user 1.

The device 10 will first be connected (step S200) to a suitable source such as to be able to subsequently receive a document. As said, this source can be any type of terminal, such as a PDA. Preferably yet, the terminal is a host, e.g., a PC connectable to a server 40 through a telecommunication network (e.g., the Internet). The device 10 can then invoke a computerized method stored thereon to trigger a trustworthy connection to the server 40, step S300. For instance, it may establish a secure communication 91 with the server over a non-secure connection 92 via the terminal 30 (e.g., upon unlocking the card).

Authenticating the device to a server can be done while initiating the communication 91 over the non-secure connection 92, e.g., by initiating a SSL/TLS authentication to the server, using user credentials as stored on the card. In this regards, setting the device in communication with the server may advantageously comprises starting, from the device, a proxy client residing at the terminal, in order for the device to connect to the server, via the terminal (note that the proxy may possibly resides on the device too). The proxy relays bits received from the device to

the internet and vice versa. Authenticating the device to the server can be achieved, e.g., bi-directionally, by initiating from the device the SSL/TLS authentication to the server.

In this respect, the memory 15'' may further have stored thereon a security software stack, including cryptographic algorithms, such as a TLS engine 14 for the SSL/TLS authentication. It may further store a USB management software (implementing a USB mass storage device or MSD profile 20), and possibly a pre-loaded networking proxy, as evoked above. As said, user credentials can be stored on the memory card (e.g., a smart card 16), such as client-server certificates (e.g., X.509) enabling TLS-client authentication. The smart card may hold sensitive personal information and have encryption means. In variants, the card cannot encrypt but is used to sign sensitive operations. In still other variants, the card is used for both encryption and signing operations. The device is preferably equipped with a standard smart card reader 17. Finally, the device has control buttons 18 (e.g., OK, Cancel, etc. selectors) and display 12, for displaying sensitive information.

Thus, in an embodiment, an SSL/TLS channel is set between the server and the device (step S300). Yet, other type of trustworthy connection can be contemplated.

A document (i.e. to be digitally signed) can now be received at the secure device 10, e.g., through the mutually authenticated connection 91 established, as evoked above. In variants, the document is trivially obtained from any other suitable source, as known.

Upon reception, the device can access (step S400) contents of the document received. Accessing contents of a file in such a device as described herein is known *per se*.

Next, the secure device may instruct to communicate the contents of the received document to an output device 12, 50 which differs from the terminal (i.e. a PC or any other insecure source), such that the contents can be subsequently verified by the user (step S500).

In a simple embodiment, the contents are displayed on a display 12 of the secure device 10. This is practical as long as the size of the document does not prevent it.

Preferably yet, the device is set in communication with an external output device 50. Then, contents of the document received can be communicated to this external device for subsequent verification. How to communicate such contents to an external device is generally known *per se*.

For example, the secure device can be configured to be connectable to a beamer (e.g., a display device with no "computing" capability, i.e., which can not be

exposed to malware), using for instance secure Bluetooth pairing (SSP), to allow the document to be verified directly from the secure device.

As another example, the secure device can else be configured to be connectable to a printer, using a USB cable or secure Bluetooth paring (SSP). This allows the document to be printed directly from the secure device (the document would not be printed via the user's PC or other device in that case).

In all cases the user can verify the contents of the document without exposing the document to a device that is not secure. Thus the user knows that the text being read and the document stored securely on its secure device are identical.

Next, the user can issue a command to sign the document. This can for instance be carried out using directly the secure device's interface (e.g., scroll wheel and buttons) or through a command issued on a connected terminal, for example a PC. In all cases, the command is ascertained (step S600) on the secure device prior to being executed, step S700. If the command is inputted directly via the secure device's interface, then the command is ascertained by default and no additional step is required. On the contrary, if the command is inputted via a connected terminal, then the command may for example be ascertained by requiring user confirmation via the secure device's interface.

Next, the actual signature can be computed directly at the secure device. In an embodiment, this can be carried out by soliciting a smart card. Yet, there is no way for a malware to alter the contents of the document being signed at the secure device. Examples of signing operations for signing data are known in the art.

Finally the signed document can be sent to a client over a suitable connection 91 established via a host, e.g. via the established connection TLS connection to the server (when the server and the client are the same). In the case where the recipient differs from the server, i.e. if the document is destined to a different location than the server, it is possible to establish a second authenticated TLS connection (or more generally a second secure connection which differs from the connection to the source of the document first sent to the secure device).

Indeed, the document does not have to originate from a secure source. For example the user may want to create the document on his/her PC and then sign and submit it. In such a case the document is created or retrieved (e.g., from the Internet) and then passed to and stored on the secure device. Furthermore, as evoked earlier, the document can simply be sent from any other sources.

Before issuing the digital signature, the user may use one of the techniques described above (beamer, printer or any output device) to verify that the document is as intended by the user. Clearly this document could have been modified by a

malware prior to being stored securely on the secure device. Yet, once the user has verified the document contents, it can be processed as described above.

Different architectures allow to implement the present invention.

1) In a first scenario, the secure device initially receives the document from a terminal, which differs from the host through which the signed document is finally sent to the recipient. Here the terminal can for example be a PC or a PDA. The document may for instance be preliminary downloaded at the terminal through an Internet query.

2) In a second scenario, the secure device initially receives the document from a server and via the host. The final recipient may be the same as the server, or not. There, two different connections can be required: a first one for initially receiving the document and a second one for sending the signed version. The two connections can even be one and a same if the final recipient is the server.

3) In a third scenario, the secure device initially receives the document from the host, i.e., a PC, but this, independently from the server evoked in the previous case. The host is then used to send the signed document to any suitable recipient.

Furthermore, it is interesting to note that aspects of the invention can advantageously used to achieve a very simple, secure method of verification of a document by a user. In particular, such a method would comprise: connecting the secure device to a host and instructing at the secure device to establish a connection between the secure device and a server, via the host (e.g. a secure connection, a mutually authenticated connection such as a TLS/SSL connection, etc., as described hereinbefore); receiving the document through the established connection; accessing (at the secure device) the contents of the document received; and instructing at the secure device to communicate the accessed contents to an external output device (as described above), such that said contents can be verified by a user.

Computer program code required to implement at least parts of the above invention may be implemented in a high-level (e.g., procedural or object-oriented) programming language, or in assembly or machine language if desired; and in any case, the language may be a compiled or interpreted language. Suitable processors include general and special purpose microprocessors. Note that instruction operations that the device, the terminal, the server or recipient performs may be stored on a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention may be performed by one or more programmable processors executing instructions to perform functions of the invention. In all case, the present invention may encompass

not only the secure device but a system including this device, augmented with one or more of the following: a terminal, at least one server or any suitable source (plus a distinct recipient of the digitally signed document, if required), and an additional device such as a printer or a beamer, for communicating contents of the document to be signed for subsequent verification by the user.

More generally, the above invention may be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them.

Generally, a processor will receive instructions and data from a read-only memory and/or a random access memory. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, flash memory devices or others.

While the present invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the present invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the present invention without departing from its scope. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed, but that the present invention will include all embodiments falling within the scope of the appended claims. For example, the device may be configured such as to prevent connection to both the PC and an external device. It may further be provided with a battery or powered by an external device.

CLAIMS

1. A method for digitally signing a document, comprising the steps of:
- providing (S100) a secure device (10), the secure device being protected against malicious software or malware, and adapted to establish a secure connection to a recipient (40) via a host, for example a personal computer or PC (30), connected to a telecommunication network;
- after connection (S200) of the secure device to a terminal (30), accessing (S400) contents of a document received at the secure device from the terminal;
- instructing (S500) at the secure device to communicate the accessed contents to an output device (12, 50) distinct from the terminal, such that said contents can be verified by a user (1);
- ascertaining (S600) at the secure device a command received to digitally sign the document and executing (S700) at the secure device the ascertained command; and
- instructing to send (S800) a digitally signed document to a recipient (40) over a connection (91) established via the host, the latter connected to a telecommunication network.

2. The method of claim **1**, wherein the terminal is the host, and wherein the method further comprises, after connecting to the host and prior to accessing the contents of the document received, a step of instructing (S300) at the secure device to establish a connection (91) between the secure device and a server (40), via the host, and receiving the document through the established connection (91).

3. The method of claim **1** or **2**, wherein a connection (91) established via the host is a secure connection.

4. The method of claim **1**, **2** or **3**, wherein:
- at the step of ascertaining (S600), the received command is a command inputted by the user at the secure device; and
- at the step of executing (S700) the ascertained command, the command executed is a command issued by the secure device and corresponding to the command inputted by the user.

5. The method of claim **1**, **2** or **3**, wherein at the step of ascertaining (S600), the received command is a command received from or through a terminal to which the secure device is connected.

6. The method of claim **2**, wherein the recipient is the server (40) and at the step of instructing to send (S800) the digitally signed document, it is instructed to send the digitally signed document to the server (40), using the same connection (91) already established with the server.

7. The method of any one of claims **1**, wherein at the step of instructing to send (S800) the digitally signed document, it is instructed to send the digitally signed document to a recipient distinct from a source of the document first received at the secure device.

8. The method of any one of the previous claims, wherein the output device is a display (12) of the secure device and the step of instructing to communicate the contents comprises:
- instructing to display the contents on the display (12) of the secure device.

9. The method of any one of the previous claims, wherein the output device (50) is an external device, the method further comprising a step of establishing a communication between the secure device and the external device (50), and wherein the step of instructing to communicate the contents comprises communicating the contents to the external device.

10. The method of claim **9**, wherein the external device (50) is a beamer, a printer or any suitable output device.

11. The method of claim **9** or **10**, wherein the step of instructing (S500) to communicate the contents comprises instructing to communicate the contents using secure Bluetooth pairing (SSP) or using a USB protocol.

12. The method of any one of the previous claims, wherein one or more secure connection established is a mutually authenticated connection such as a TLS/SSL connection.

13. A secure device (10) having processing means (15), a memory (15', 15'') and interfaces (17, 18, 20), configured to couple to or interact with:
- a user (1);
- a terminal such as a personal computer or PC (30), and
- a recipient (40), the secure device configured to establish a secure connection such as a TLS/SSL connection with a recipient (40) via a host (30) when the secure device

is connected to the host and the latter is arranged to communicate with the recipient through a telecommunication network,
and further comprising a computerized method stored on the memory and executable by the processing means for executing all the steps of the method according to claims **1** to **12**.

14. A system comprising:
- the secure device (10) of claim 12;
- a personal computer or PC (30); and
- a server (40).

15. A computer program product comprising instructions executable by processing means for executing all the steps of the method of claims **1** to **12**.

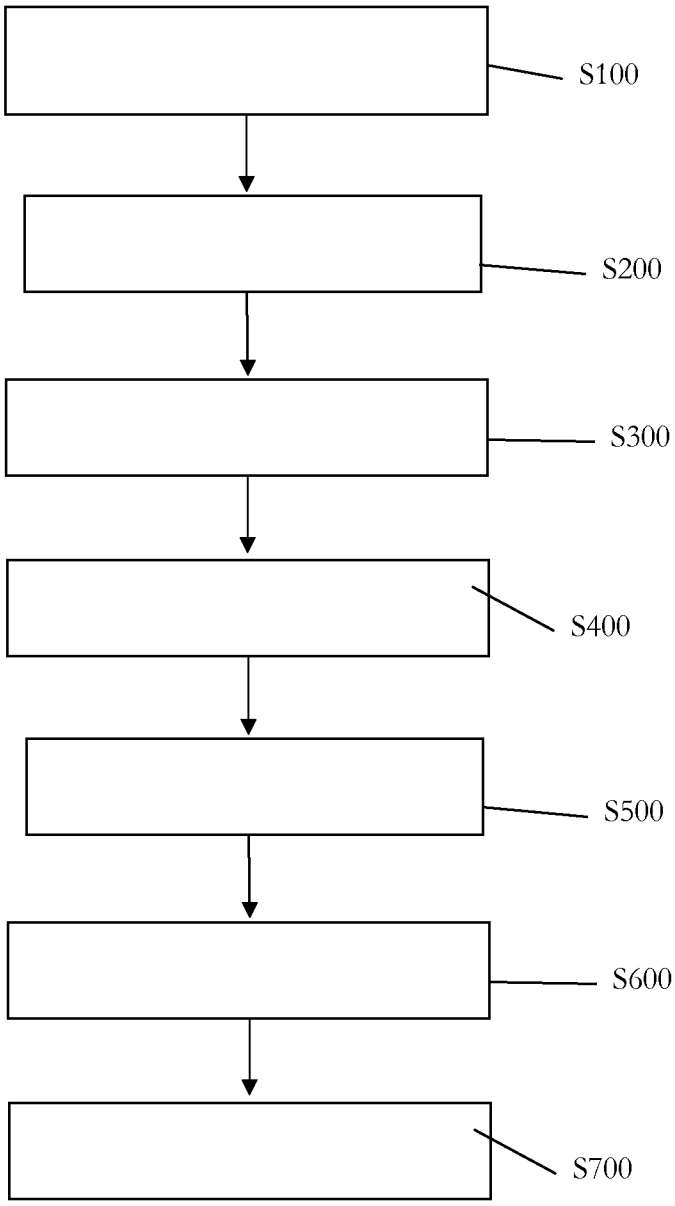


FIG. 1

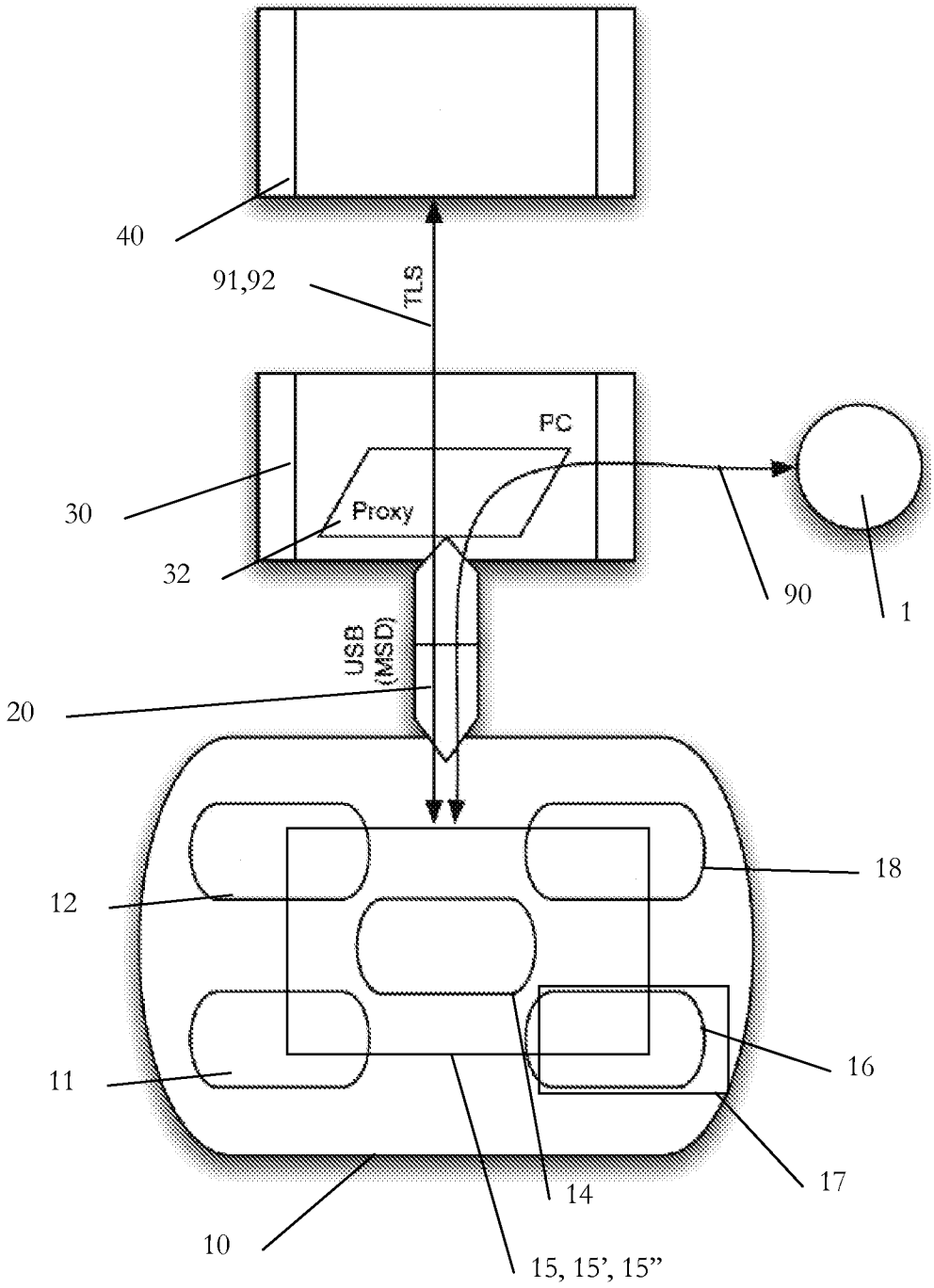

40
91,92
TLS
PC
Proxy
30
32
90
1
USB (MSD)
20
18
12
16
11
17
14
10
15, 15', 15"

FIG. 2

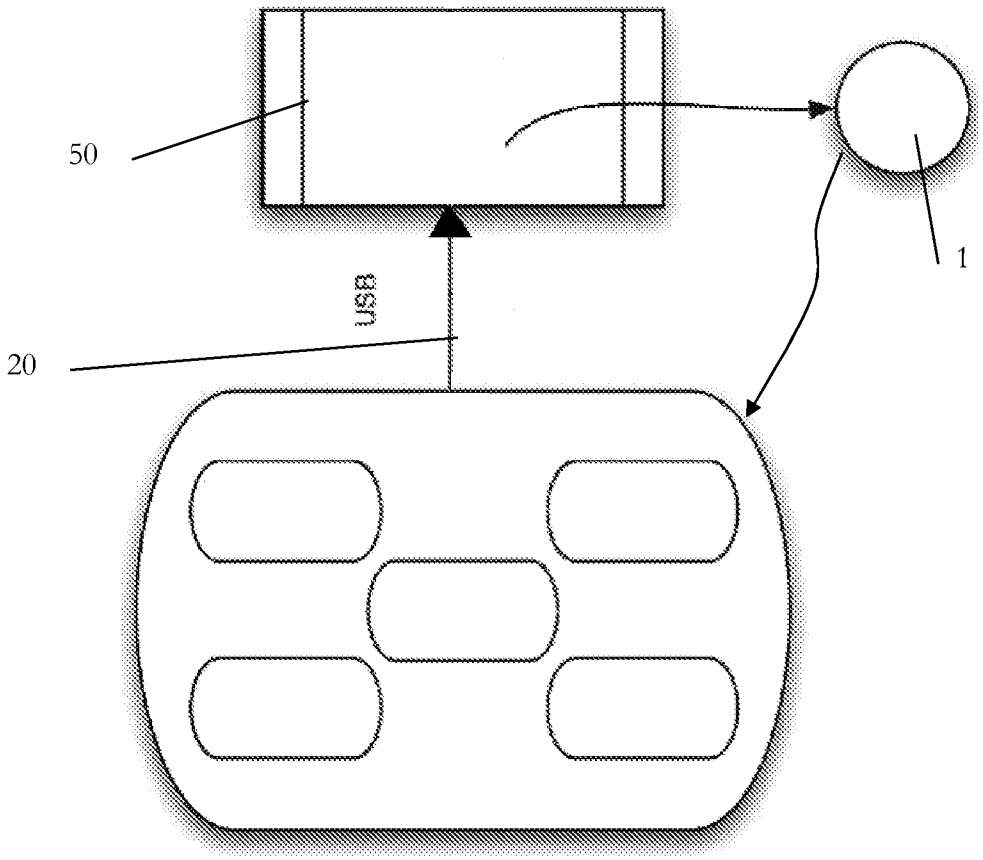


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2011/051321

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
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 practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/044639 A2 (GEMPLUS CARD INT [FR]; BOIS DANIEL [FR]; GAUTERON LAURENT [FR]; GIRAUD) 30 May 2003 (2003-05-30) the whole document	1-15
X	WO 01/46785 A2 (SCM MICROSYSTEMS GMBH [DE]; HEINS KERSTEN W [DE]) 28 June 2001 (2001-06-28) the whole document	1-15
A	GB 2 267 986 A (ALGORITHMIC RES LTD [IL]) 22 December 1993 (1993-12-22) the whole document	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier 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	Date of mailing of the international search report
27 July 2011	04/08/2011

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2011/051321

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03044639 A2	30-05-2003	AU 2002356250 A1	10-06-2003
		FR 2832522 A1	23-05-2003
WO 0146785 A2	28-06-2001	DE 19961838 A1	05-07-2001
		EP 1240569 A2	18-09-2002
		US 2003140229 A1	24-07-2003
GB 2267986 A	22-12-1993	DE 69333122 D1	04-09-2003
		DE 69333122 T2	15-04-2004
		EP 0587375 A2	16-03-1994
		IL 103062 A	04-08-1996
		SG 43927 A1	14-11-1997
		US 5406624 A	11-04-1995