PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00	A1	(11) International Publication Number: WO 98/08325
		(43) International Publication Date: 26 February 1998 (26.02.98)

(21) International Application Number: PCT/US97/14571

(22) International Filing Date: 20 August 1997 (20.08.97)

(30) Priority Data:
60/023,352 20 August 1996 (20.08.96) US

(71) Applicant *(for all designated States except US)*: ASCOM HASLER MAILING SYSTEMS INC. [US/US]; 19 Forest Parkway, Shelton, CT 06484-6140 (US).

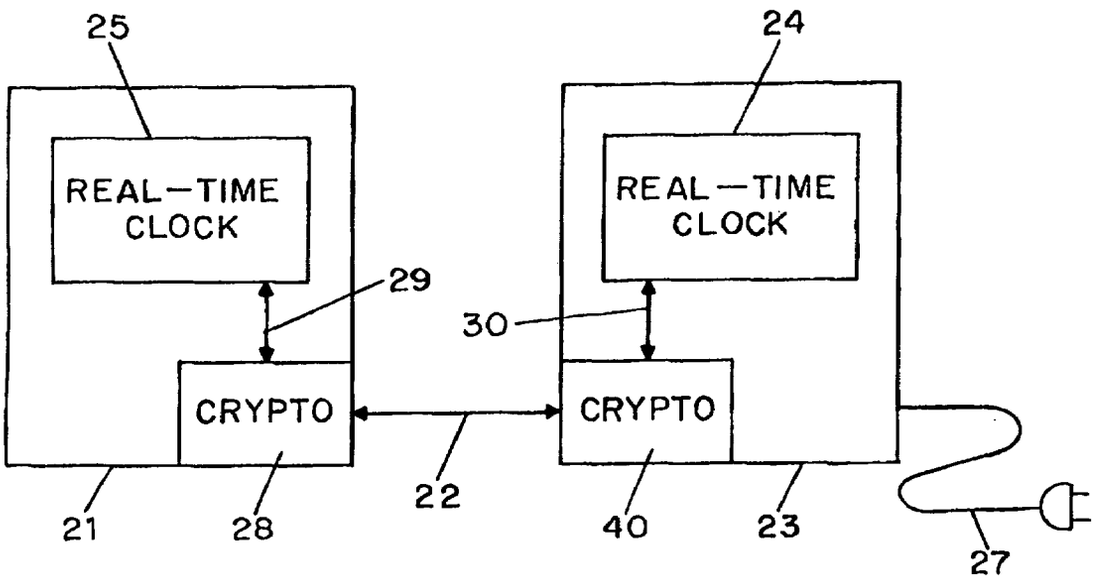
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BROOKNER, George [US/US]; 11 Surrey Drive, Norwalk, CT 06851 (US). BROWN, Michael [US/US]; 84 Field Street, Norwalk, CT 06851 (US). ESKANDARI, Fetneh [IR/US]; 166 Dore Lane, Middletown, CT 06457 (US). SCHWARTZ, Robert [US/US]; 191 Linden Avenue, Branford, CT 06405 (US).

(74) Agent: OPPEDAHL, Carl; Oppedahl & Larson, 1992 Commerce Street #309, Yorktown Heights, NY 10598-4412 (US).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: PRINTING POSTAGE WITH CRYPTOGRAPHIC CLOCKING SECURITY



(57) Abstract

Secure activities are carried out between a client (23) and a server (28) in connection with the printing of postage. A cryptographically secure exchange (22) is employed so as to establish a common time base (24, 25), said common time base obviating a constant (e.g. battery) power supply. The postage-printing client (23) thus need not have a reliable power supply in the absence of AC (mains) power.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

PRINTING POSTAGE WITH CRYPTOGRAPHIC CLOCKING SECURITY

Technical field

The invention relates generally to establishing conditions for secure activities between a client and a server in connection with the printing of postage, and relates specifically to printing postage employing a cryptographically secure exchange to establish a common time base, said common time base obviating a constant (e.g. battery) power supply.

Background art

If one takes into account the many constraints (cost, post office approval, customer requirements, mechanical requirements, human readability) that must be simultaneously satisified, it may fairly be said that it is not easy to print postage. For nearly a hundred years, companies such as Hasler (a predecessor of the assignee of the present invention) and its competitors have provided postage meters which print postage by means of mechanical relief die plates. Generations of mechanical engineers have developed and refined the art of mechanical printing of postage so that today's postage meters (also called franking machines) offer a high-quality die-printed postage indicium together with the all the benefits flowing from the use of microprocessors.

It has been recently suggested to use digitally formed indicia instead of die-printed indicia, a move which would discard a substantial fraction of the accumulated experience with die printing of postage and which opens up a host of new problems. The printing technologies most often proposed for digitally formed indicia are ink-jet and laser printing. These technologies have many potential disadvantages. Among them is that if the postal indicia are to be printed with an off-the-

shelf printer connected to a postal security device via a nonsecure data link, then encrypted information must be printed within the indicia to assist in distinguishing between authentic and fraudulent indicia. The encrypted information is generated by cryptographic apparatus within the postal security device.

It is considered desirable, and is known in the art, to provide time and date information as inputs to the cryptographic apparatus within the postal security device (PSD or client). The encrypted information from the PSD is applied to a mail piece in the postal indicia. Such information is more helpful to the post office for authentication purposes than an indicium that lacks any encrypted information containing time/date information.

At least one postal authority has suggested that it is preferable to have, within the postal security device, a time base that is powered by a reliable power supply that is provided without interruption even when AC (mains) power is removed. With such a device, even when the power is turned off or disconnected by a user (or is lost due to a utility power outage) the time base or real-time clock is continuously running, consuming power from the internal reliable power supply.

For the internal time base to be of any meaningful help for authentication purposes, it must be quite accurate, typically requiring an accuracy better than that of a consumer wristwatch. Such a time base generally relies upon a crystal oscillator, and the crystal for this purpose is more expensive than the inexpensive crystal used in a consumer wristwatch. The high-accuracy time base and internal reliable power supply all add to the cost of the postal security device.

Such a system generally relies on the internal power source working without interruption, and in the event of loss of the internal power source, a variety of manual steps are generally required to restore normal function, steps including taking the postal security device out of service. Such steps are at best annoying to the user, and may be very disruptive for the user.

It would be desirable to reduce the cost of the postal security device, to make it less likely to require being taken out of service, and yet to maintain the authentication benefits that come from the use of a consistent time base that matches the rest of the system.

Disclosure of invention

Secure activities are carried out between a client and a server in connection with the printing of postage. A cryptographically secure exchange is employed so as to establish a common time base, said common time base obviating a constant (e.g. battery) power supply. The postage-printing client thus need not have a reliable power supply in the absence of AC (mains) power.

Brief description of drawing

The invention will be described in connection with a drawing in several figures, of which:

Fig. 1 shows a prior-art arrangement of a postal security device together with a system;

Fig. 2 shows a arrangement of a postal security device together with a system in accordance with the invention;

Fig. 3 shows a prior-art exchange of messages between a client and server;

Fig. 4 shows an exchange of messages between a client and server in accordance with the invention;

Fig. 5 shows a prior art time line depicting time correspondence between a client postal security device and server;

Fig. 6 shows a time line depicting time correspondence between a client postal security device and server according to the invention; and

Fig. 7 shows a postage printing apparatus in accordance with the invention, including a postal security device.

Modes for Carrying out Invention

Fig. 1 shows a prior-art arrangement of a postal security device together with a system. Postal security device (client) 23 is used to print postage by means of an off-the-shelf printer (omitted for clarity in Fig. 1). Power is provided by AC (mains) power cord 27. A real-time clock 24 keeps highly accurate time, and is sustained in the absence of external power by means of internal reliable battery or other power source 26. From time to time, the client 23 is in communication over nonsecure channel 22 with a server 21, for example for resetting the client 23 to contain more postage value. Real-time clock 25 is presumed to be highly accurate. Because the number of servers 21 is very small (in contrast to the large number of clients 23), the high cost of the highly accurate real-time clock 25 is not a problem. Indeed the distinction is not so much between the client 23 and the server 21, as it is a distinction between the client 23 and

the rest of the world, including the apparatus (omitted for clarity in Fig. 1) used by the postal authorities to authenticate postal indicia. The numerous such apparatus are all capable of receiving trustworthy time and date information since they are all physically controlled by the postal authority. As noted above, however, the PSD clients 23 are not physically controlled by the postal authorities, and they are great in number, thus prompting the prior-art assumption that the only workable way of providing a time standard for use in the clients 23 is by means of an internal reliable power supply and highly accurate time base.

Fig. 2 shows a arrangement of a postal security device together with a system in accordance with the invention. In this arrangement, as in the prior art, the client PSD 23 has a real-time clock. But importantly, upon power-up of the PSD 23, or at some time thereafter, the PSD conducts a cryptographically secure communication via nonsecure channel 22 with a trusted time base, here presumed to be within server 21. The communication may be desirably be cryptographically secure as set forth in FIPS PUB 140-1, but preferably one skilled in the art can select a level of cryptographic security appropriate to the needs of the particular system. The assumption is that the trusted time base (clock 25 in Fig. 2) is a certified trusted third party, certified by the postal authority both as to the accuracy of its time information as as to the desired level of security of the cryptographic exchange used to communicate the time information to the client 23.

The certified real-time clock could be operated by the manufacturer (vendor) of the postal security devices or by the postal service, or by third parties.

Those skilled in the art will appreciate that many

communications channels 22 would serve the desired purpose, including Internet TCP/IP connectivity between the client 23 and a certified real-time clock. In a typical system, the postal security device would be employed in a business premises with a local area network that is TCP/IP-connected with the Internet, and the PSD would have an ethernet interface permitting it to be plugged into the local area network. In this way, there would be no need for a dedicated telephone line for modem-based communications. Such a configuration offers the further benefit that external devices (e.g. from the manufacturer of the PSD or the postal authorities) could initiate communications for a variety of purposes.

Turning now to Fig. 7, there is shown a postage printing apparatus in accordance with the invention, including a postal security device 23. The cryptographic apparatus 40 is used to generate the encrypted indicia that are printed on the printer 42. The communications channel 41 between the PSD 23 and the printer 42 is presumed to be nonsecure. A postage value register 59 contains information about the amount of postage value printed or available to be printed. If the available postage is exhausted (i.e. the postage meter is empty) then no indicia are printed at the printer 42.

Returning to Fig. 3, there is shown a prior-art exchange of messages between a client and server. The server 21 and client 23 are presumed to have nearly the same time (t21-1 and t23-1, reference numeral 30) because each has a very accurate clock. With times thus synchronized, an exchange of data packets 31, 32, 33, and 34 may take place from time to time, for example to reset the PSD client 23 to contain more postage value, or for other purposes such as collection of statistical data. Also from time to time an encrypted message 51 is passed to the nonsecure printer (omitted for clarity in Fig.

3) and is printed on a mail piece. Data packets 31-34 pass over nonsecure channel 22 as described above. The packet exchanges may for example be those described in US Pat. No. 5,237,506, owned by the present applicant.

Fig. 4 shows an exchange of messages between a client and server in accordance with the invention. In this arrangment, it is understood that the PSD 23 has been powered up, and does not know what time it is, as depicted by the question mark in Fig. 4 (reference numeral 35). Then, in some exchange of packets such as 31A, 32A in Fig. 4, a cryptographically secure communication occurs in which the presumed accurate time t21-1 is communicated to the client PSD 23. The PSD 23 loads the time into its time base and the time is used in subsequent cryptographic activities such as the printing of a postal indicia in data item 51.

Fig. 5 shows a prior art time line depicting time correspondence between a client postal security device and server. The real-time clocks of the PSD client 23 and the trusted time base of the server 21 are synchronized once at time 57, perhaps at the time of manufacture. Thereafter, the authentication activities undertaken by the postal authorities assume that subsequent events are simultaneous as depicted by vertically aligned event ticks in Fig. 5.

Fig. 6 shows a time line depicting time correspondence between a client postal security device and server according to the invention. In this time line, there are periods of time during which no external power is applied to the PSD client 23 and it has no continuous timekeeping by its internal time base. Instead, from time to time the secure synchronization takes place (shown by events 31A) as discussed above. The result is that the time bases of the client 23 and the presumed correct server 21 are more nearly in synchronization.

It will be recalled that the cryptographic secure time base communication permits the use, within the postal security device, of a time base that need not be as accurate (and expensive) as the highly accurate time base that would be called for in a prior art system. In the embodiments previously described, a time synchronization takes place at least as often as once per application of AC (mains) power to the postal security device. It must be appreciated, however, that time drift thereafter (while AC power continues to be present) may lead to a condition in which the client time value differs unduly from that of the rest of the world (and of the server time source). Thus, it is desirable to provide an optional functionality in that the PSD may keep record of the number of franking events (printings of postage) since the last cryptographic exchange in which the time was synchronized with the trusted standard. When some number of frankings has occurred (e.g. fifty), the PSD may be programmed to require that another cryptographically secure time synchronization be performed before any further frankings will be done. Alternatively, it may be desirable to configure the PSD so that when some interval of time has passed, the PSD will require that another cryptographically secure time synchronization be performed before any further frankings will be done. In this way, the cost of the PSD may be further reduced in that the time base within the PSD need not be highly accurate but need merely have small enough drift that the accumulated error will be small within the preset number of frankings or the preset time interval.

Claims

1. A system for printing postage indicia, said system comprising first and second apparatus, said second apparatus connected via a nonsecure link to a printer printing said indicia, said second apparatus powered by interruptable external power, said second apparatus comprising a second time base functioning only in the presence of said external power, said first apparatus comprising a trusted first time base, said second apparatus further comprising a register indicative of postage value printed at said printer, said indicia containing encrypted information based at least upon the contents of the register and upon the contents of the second time base, said second time base synchronized with said first time base by means of a cryptographically secure communication subsequent to provision of said external power to said second apparatus.

2. The system of claim 1 wherein the synchronization is repeated after a predetermined number of indicia are printed and before any subsequent indicia are printed.

3. The system of claim 1 wherein the synchronization is repeated after a predetermined interval of time has elapsed and before any subsequent indicia are printed.

4. A method for use with first and second time bases for printing of postage indicia at a printer, said indicia containing encrypted information based at least upon the contents of a register indicative of postage value printed at the printer, and upon the contents of the second time base, the method comprising the steps of: applying power to the second time base, synchronizing the second time base to the first time base via a cryptographically secure communication between the first and second time bases,

calculating the encrypted information, communicating the encrypted information to the printer, and printing the indicia at the printer.

5. The method of claim 3 wherein the synchronization is repeated after a predetermined number of indicia are printed and before any subsequent indicia are printed.

6. The system of claim 3 wherein the synchronization is repeated after a predetermined interval of time has elapsed and before any subsequent indicia are printed.

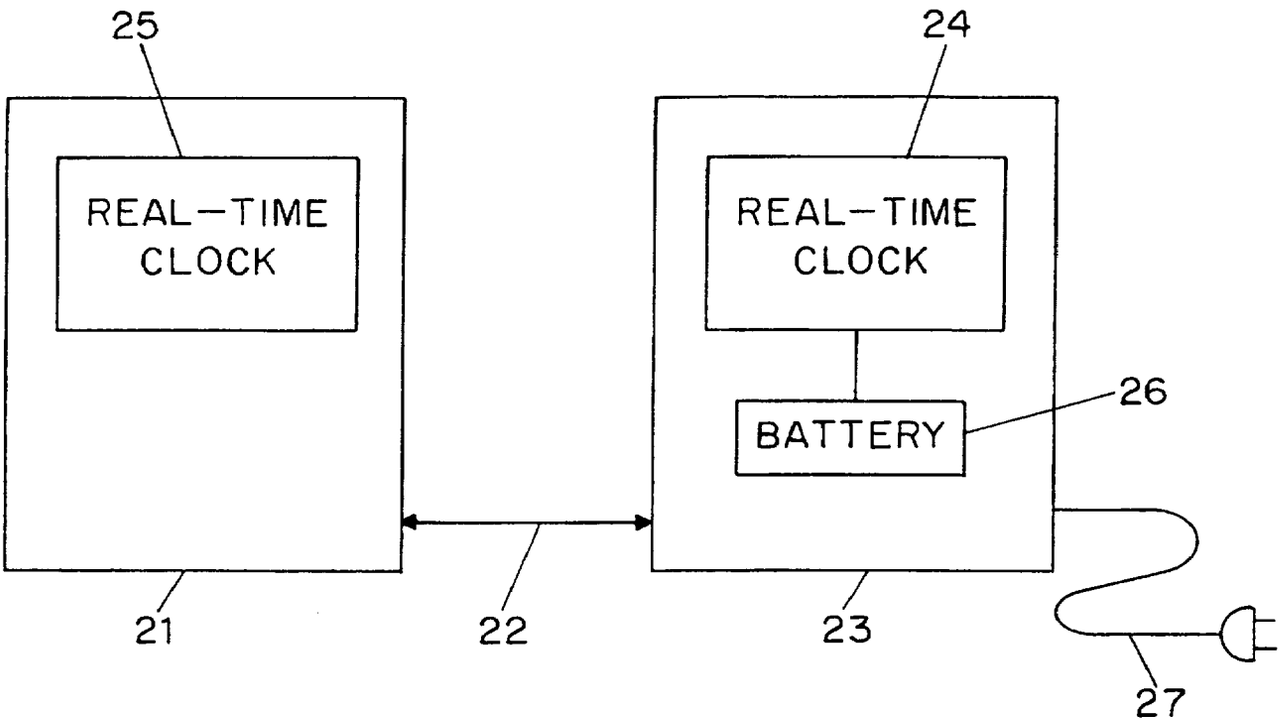


FIG. 1 PRIOR ART

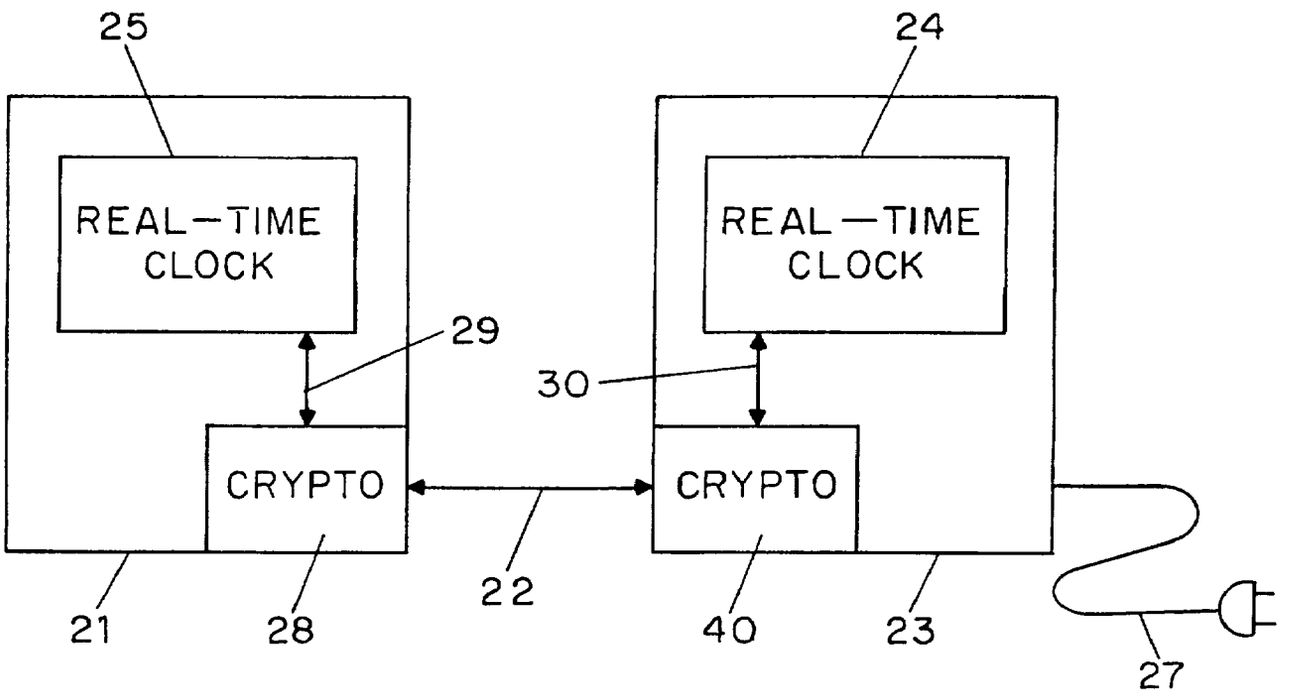


FIG. 2

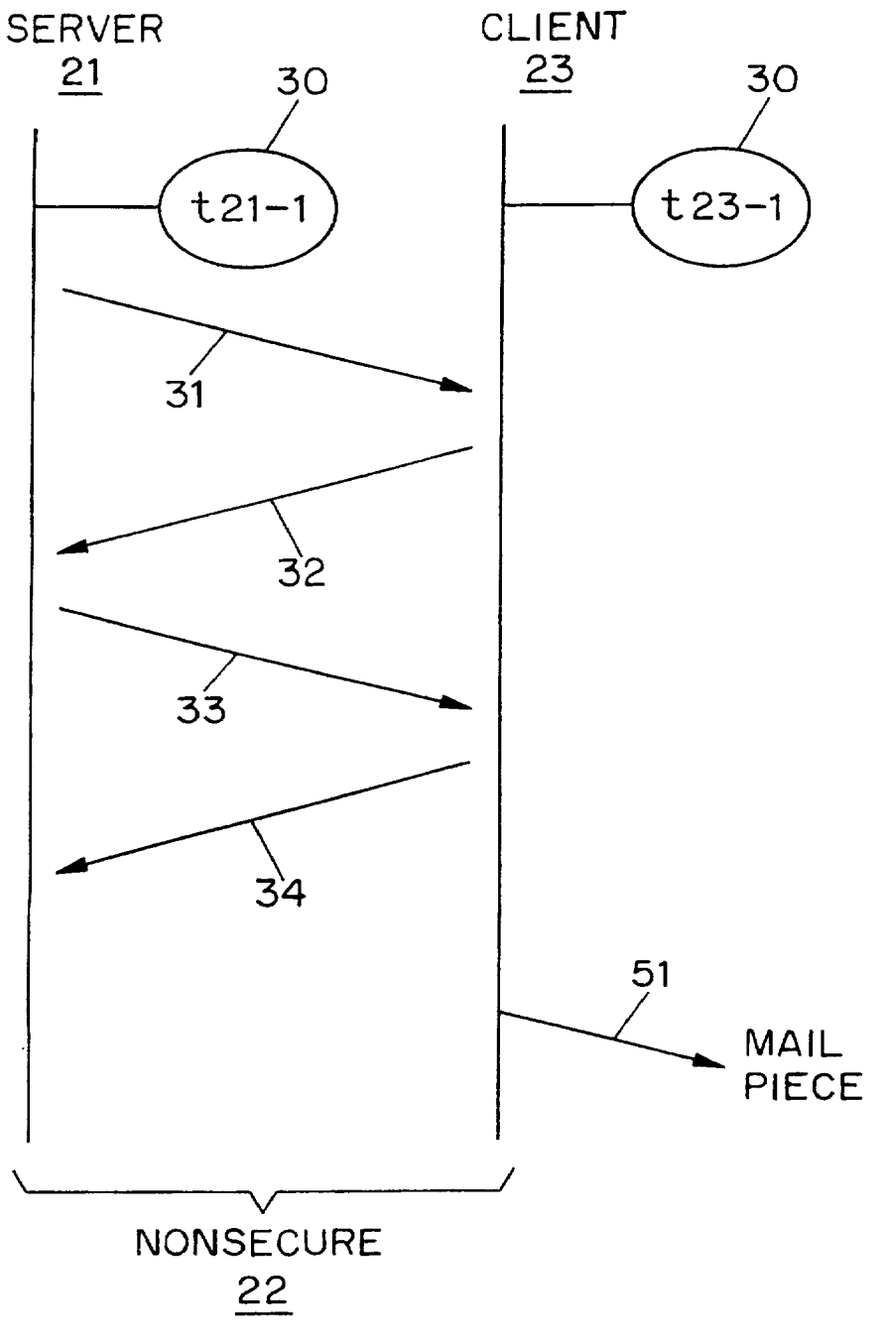


FIG. 3
PRIOR ART

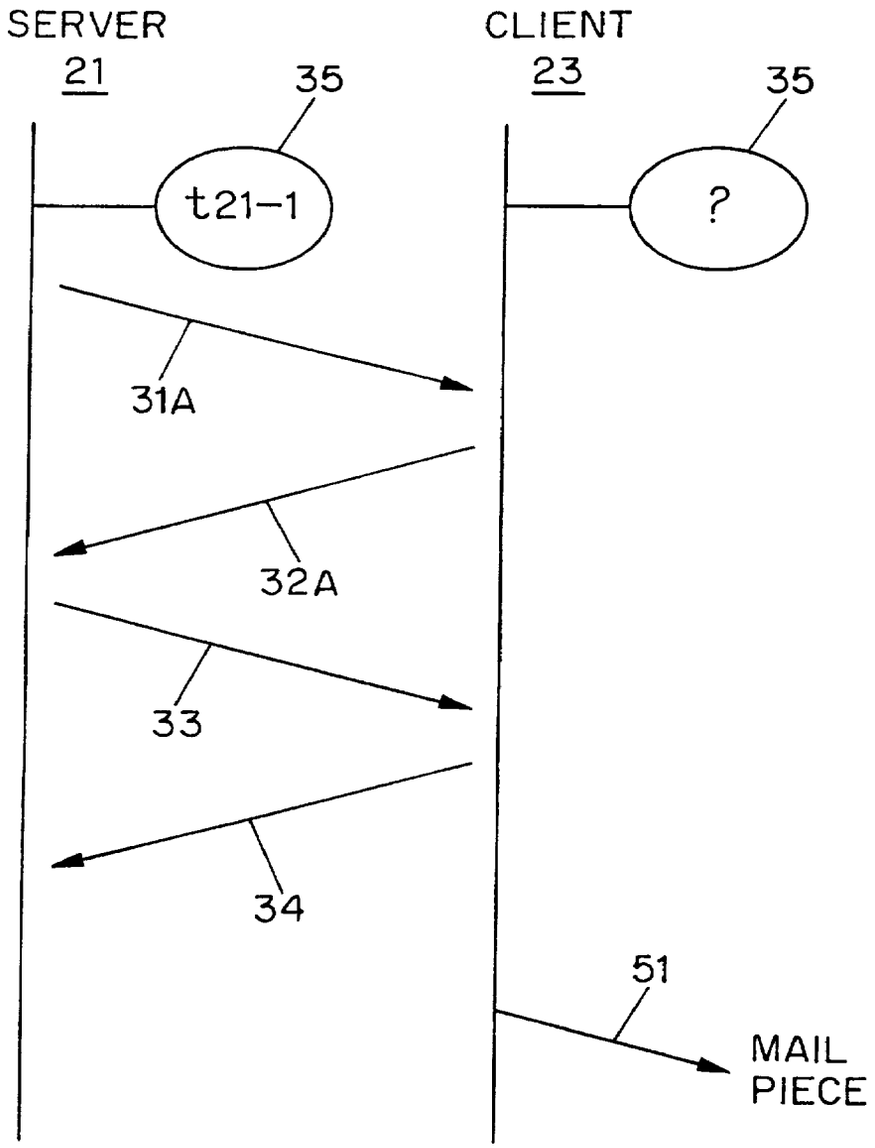


FIG. 4

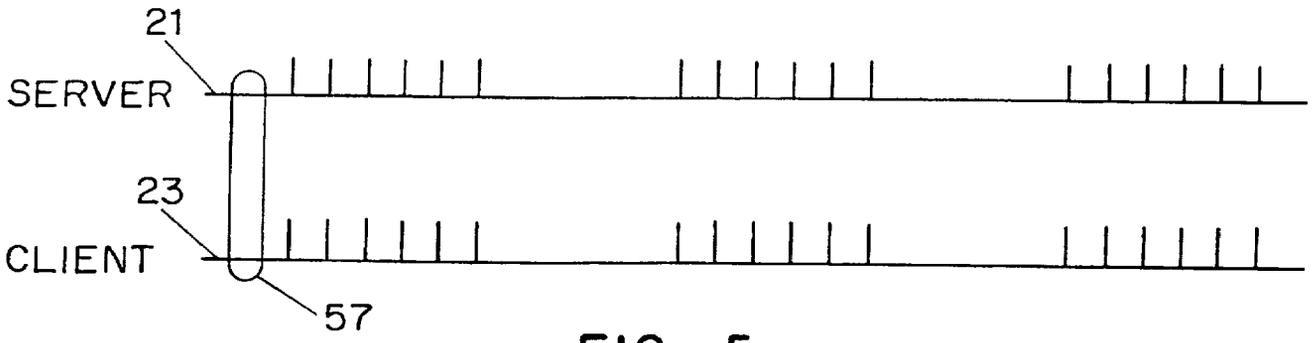


FIG. 5
PRIOR ART

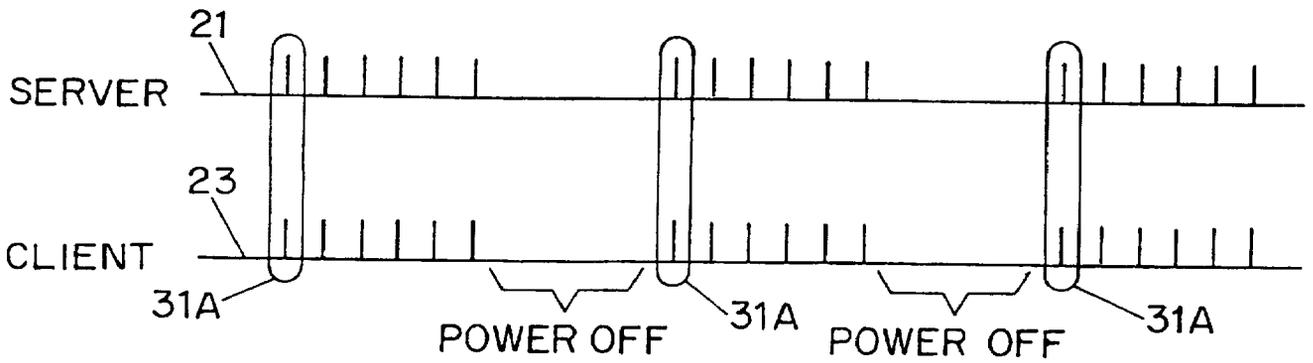


FIG. 6

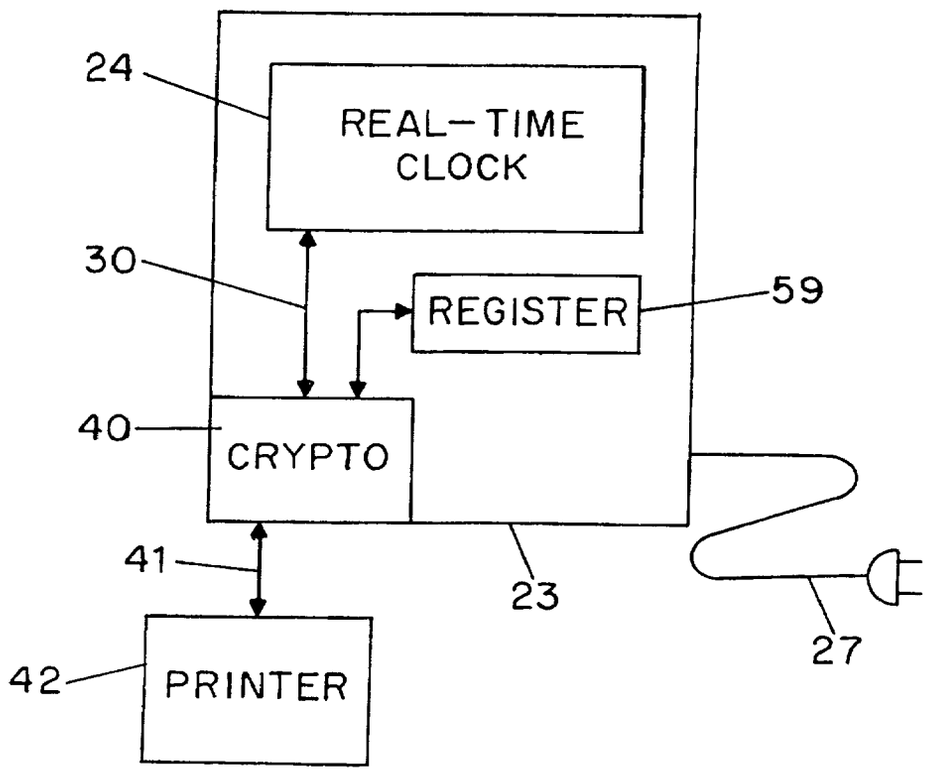


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/14571

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL :380/51
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)

U.S. : 380/25, 30, 51

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,725,718 A (SANSONE ET AL) 16 February 1988, see figures 1 and 5A.	1-6
Y	US 4,757,537 A (EDELMANN ET AL) 12 July 1988, see figure 5.	1-6
Y	US 4,775,246 A (EDELMANN ET AL) 04 October 1988, see figures 8 and 9.	1-6
Y	US 4,868,877 A (FISCHER) 19 September 1989, see figure 2.	1-6
Y	US 5,001,752 A (FISCHER) 19 March 1991, see entire document.	1-6
Y	US 5,022,080 A (DURST ET AL) 04 June 1991, see figure 1.	1-6

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search
21 NOVEMBER 1997

Date of mailing of the international search report
14 JAN 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
SALVATORE CANGIALOSI
Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/14571

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,022,080 A (DURST ET AL) 04 June 1991, see figure 1.	1-6
Y	US 5,444,780 A (HARTMAN, JR.) 22 August 1995, see figures 1 and 2.	1-6