PCT
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 12/14

A1

(11) International Publication Number: WO 92/12485

(43) International Publication Date: 23 July 1992 (23.07.92)

(21) International Application Number: PCT/US91/09270

(22) International Filing Date: 10 December 1991 (10.12.91)

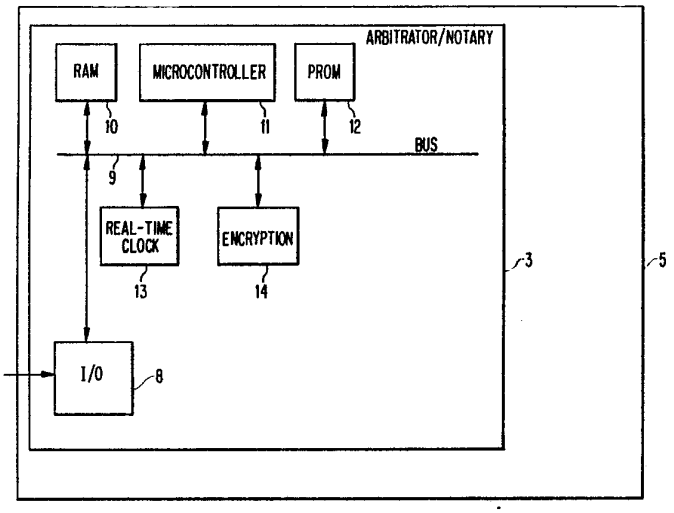
(30) Priority data:
637,675 7 January 1991 (07.01.91) US

(71)(72) Applicant and Inventor: BLANDFORD, Robert, R. [US/US]; 1809 Paul Spring Road, Alexandria, VA 22307 (US).

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

Published
With international search report.

(54) Title: DEVICES TO (1) SUPPLY AUTHENTICATED TIME AND (2) TIME STAMP AND AUTHENTICATE DIGITAL DOCUMENTS



(57) Abstract

A digital system, called a notary, designed to (1) provide authenticated time and/or (2) to time stamp and authenticate digital documents, comprising a clock and digital circuits. The clock uses a power-supply system designed to avoid failure, and the notary stops functioning should any failure of the clock or power source be detected. The time and/or document is authenticated by a secret key in the digital circuit which is inaccessible from outside the notary. The system is sealed so that the clock time may not be changed or the secret key discovered without detection. The security and usefulness of the system rests on the integrity of this seal. A user may supply a digital signature and sequence number to be authenticated so that it may later be verified that the user archived the document at the time stamped so that missing documents in a file may be identified. The notary also may supply an identification number and sequence number to be authenticated with the time and/or document to identify the notary and to detect deletion of documents and/or possible excessive use of the notary. A mode of operation of the notary is available in which it computes a standard format of a document before authentication so that copies of the document made by different methods, e.g. handwritten facsimiles, may also be authenticated. The system may be used in conjuction with a computer to ensure that the computer is booted with the correct time. Using either private or public key techniques, the time and/or documents may be verified without direct access to the secret key.

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.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CS	Czechoslovakia
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GN	Guinea
GR	Greece
HU	Hungary
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
PL	Poland
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

DEVICES TO (1) SUPPLY AUTHENTICATED TIME AND (2) TIME STAMP AND AUTHENTICATE DIGITAL DOCUMENTS

BACKGROUND OF THE INVENTION

This invention relates to devices and means, at least partly in hardware (1) to provide authenticated time to a computer or other user; and (2) to assure that a specified digital document did in fact originate with a particular person and was stamped at a particular time and in a particular order by a particular device (the "arbitrator" or "notary");

In recent years there have been many articles in the trade and popular press describing incidents in which computer records have been erased or altered illegally.

Computer records are particularly liable to such alteration; they can be less secure in this respect than are paper records because an altered paper record may reveal erasures. Even if a paper record is created from scratch, the age of the paper or ink on a single sheet of paper, or progressively in a bound notebook, may reveal the forgery. Such aging does not occur for computer records. And, of course, handwriting or other forensic analysis may reveal that a paper document was signed by other than the nominal author.

Even permanent records on such WORM devices as optical disks may be read and re-written, possibly with falsified dates, on a fresh disk after making desired alterations.

This, and many other falsification techniques available, for example, to a superuser or other "owner" of a computer system would be made more difficult if all computers were required by hardware to access an authenticated source of time in order to set the system clock.

From a positive point of view, it would be desirable if computer records could take the place of paper records for legal purposes, thus minimizing the large volume of stored paper.

As another use, a person keeping a diary would like to be sure that the record, once committed to the permanent computer recording device cannot be undetectably altered, even by himself.

In these cases it may be important that archived records be traceable to the person who actually created them, that the records be unaltered, unalterably time-stamped and sequenced, that it be clear which physical device (the "notary") actually performed the time stamping and authentication, and that access to the records be controlled by passwords and other means.

It would also be desirable if paper copies of the original digital records could be certified as authentic; i.e. that it could be verified that each copy was archived by a particular person on a particular machine at the indicated time. It would also be desirable if it could be shown that no documents are missing from a nominally complete file of the paper records.

In the present invention these goals are achieved by the use of a sealed digital processing circuit, called an arbitrator (or "notary"), which contains a real-time clock which either can not be reset, or can be reset only under strict procedures, and an authentication circuit which can compute digital signatures using a secret key, inaccessible from outside.

For the purpose of (1) providing authenticated time, the first aspect of the invention, the arbitrator computes an authentication check (signature) over the time from the sealed clock and the arbitrator's identification number (ID) and upon request returns the time and signature to the user. If the signature was

computed using private key techniques then the user or other verifier may validate the signature by recomputing the signature with a supplemental device which also contains the secret key in an inaccessible form. This would, of course, be preferable to allowing the user to have direct access to the secret key, since this would enable him to falsify the signature. Many other methods for generating and validating signatures using private keys may be found in the open cryptographic literature.

If the signature of the time and ID was computed using public key techniques then the verification of the signature may be performed using the public key without any form of access to the secret key.

In some applications the user may want to ensure that the time and authenticating signature received is not simply a copy of a previous message. This can be assured by the user generating and sending to the arbitrator a random number which the arbitrator then appends to the time from the sealed clock before computing the digital signature. The signature then verifies that the time was not authenticated before the random number was generated.

For the purpose of (2) authenticating documents, a second aspect of the invention, the arbitrator computes a signature over the full text of the document (or in some cases preferably of a hash of the full text of the document), a sequence number provided by the user, the user's digital signature, the internal clock time, the arbitrator's ID, and the arbitrator's sequence number. The arbitrator then returns this signature to the outside where it can be verified using the public key and compared to the original.

In order to provide background information so that the invention may be completely understood and appreciated in its proper context, reference is made to a prior art patent application and to a publication in methods of time-stamping digital documents as follows:

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.