METHOD AND APPARATUS FOR SELF-AUTHENTICATING DIGITAL RECORDS

500

USER-2 SIGNS D1, D2, ..., Dn TO FORM SD1, SD2, ..., SDn

502

USER-2 HAS EACH OF SD1, SD2, ..., SDn TIMESTAMPED

504

USER-2 GATHERS CERTIFICATE AND CRL INFORMATION IN ITS CHAIN AND HAS IT TIMESTAMPED

506

USER-2 SENDS TIMESTAMPED SD1 ALONG WITH TIMESTAMPED CERTIFICATE AND CRL INFORMATION TO USER-1

508

Abstract: A method for proving the validity of a record digitally signed by a user having a digital certificate issued by a certification authority within a hierarchy of certification authorities. The user signs the record (502), and obtains the digital certificates and certificate revocation information for all the certification authorities in the chain of the hierarchy extending from the user to the root certification authority. A timestamp is applied to the record (506), the digital certificates and the certificate revocation information to establish a point in time in which all items were created, current and valid. If, at some later point, one or more of the digital certificates either expire or are revoked, the timestamp serves as evidence of the integrity of the signed record.
Published:
— with international search report

(88) Date of publication of the international search report: 28 March 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(7) : H04L 9/00  
US CL : 713/156, 157, 158

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.: 713/156, 157, 158

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)

EAST: search terms: "haber.in. and ((time adj stamp$3) or (timestamp$3))"

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>US 5,903,882 A (ASAY et al) 11 May 1999 (11.05.1999), see Figs. 8 and 9 and column 2, lines 57-67 and column 41, lines 10-41.</td>
<td>1-29</td>
</tr>
<tr>
<td>Y</td>
<td>US 5,136,646 A (HABER et al) 04 August 1992 (04.08.1992), see abstract.</td>
<td>1-29</td>
</tr>
<tr>
<td>A</td>
<td>US 5,373,561 A (HABER et al) 13 December 1994 (13.12.1994), see Fig. 2 and abstract.</td>
<td>1-29</td>
</tr>
<tr>
<td>A</td>
<td>US 5,687,235 A (PERLMAN et al) 11 November 1997 (11.11.1997), see abstract.</td>
<td>1-29</td>
</tr>
<tr>
<td>A</td>
<td>US 5,745,574 A (MUTFIC) 28 April 1998 (28.04.1998), see Figs. 1A, 1B, and 6.</td>
<td>1-29</td>
</tr>
<tr>
<td>A</td>
<td>US 5,903,651 A (KOCHER) 11 May 1999 (11.05.1999), see abstract and Fig. 6.</td>
<td>1-29</td>
</tr>
</tbody>
</table>

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

Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance  
- "E" earlier application or patent published on or after the international filing date  
- "L" document which may throw doubts on priority claims 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

Date of the actual completion of the international search: 17 September 2001 (17.09.2001)

Date of mailing of the international search report: 02 JAN 2002

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:  
Albert DeCady  
Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)