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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2002 (03.10.2002)

PCT

(10) International Publication Number
WO 2002/078238 A3

(51) International Patent Classification:
G06F 17/30 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/US2002/010030

(22) International Filing Date: 27 March 2002 (27.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/279,287	27 March 2001 (27.03.2001)	US
60/306,490	18 July 2001 (18.07.2001)	US
60/309,340	31 July 2001 (31.07.2001)	US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, WA 98052 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BOYEN, Xavier** [Stateless/US]; 1939 Rock Street, #19, Mountain View, CA 94043 (US). **QIAN, Zhenyu** [Stateless/US]; 11592 Bridge Park Ct., Cupertino, CA 95014 (US). **TEODOSIU, Dan** [US/US]; 4151 #E El Camino Way, Palo Alto, CA 94305-4035 (US).

(74) Agents: **CONKLIN, John, B.** et al.; Leydig, Voit & Mayer, LTD, Suite 4900, Two Prudential Plaza, 180 North Stetson, Chicago, IL 60601-6780 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

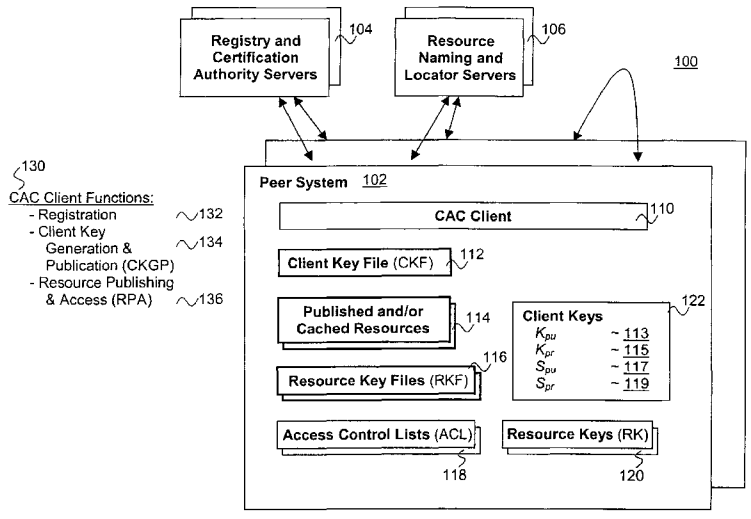
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) Title: DISTRIBUTED, SCALABLE CRYPTOGRAPHIC ACCES CONTROL



(57) Abstract: Published resources are made available in an encrypted form, using corresponding resource keys, published through resource key files, with the publications effectively restricted to authorized peer systems (102) only by encrypting the resource keys in a manner only the authorized peer systems are able to recover them. In one embodiment, the resource keys (120) are encrypted using encryption public keys of the authorized peer systems or the groups to which the authorized peer system are members. In one embodiment, the encryption public keys of individual or groups of authorized peer systems are published for resource publishing peer systems through client (112) and group key files respectively. Group encryption private keys are made available to the group members through published group key files. Further, advanced features including but not limited to resource key file (116) inheritance, password protected publication, obfuscated publication, content signing, secured access via gateways, and secured resource search are supported.

WO 2002/078238 A3

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(88) Date of publication of the international search report:
18 October 2007

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

International application No.
PCT/US02/10030

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 17/30; H04L 9/00
US CL :707/200, 202; 713/165, 185, 201
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. : 707/200, 202; 713/165, 185, 201

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)

West, East, Web

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 6,351,813 B1 (Mooney et al.) 26 February 2002, see abstract	1-42, 66-107, 46-54, 111-119, 64-65, 129-130
A, P	US 6,249,866 B1 (Brundrett et al.) 19 June 2001, See abstract.	43-45, 108-110, 55-63, 120-128

☐ 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 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 MAY 2002	Date of mailing of the international search report 28 JUN 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 for SANJIV SHAH James R. Matthews Telephone No. (703) 305-8355

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/10030

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/10030

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim(s)1-42, 66-107, 46-54, 111-119, drawn to an access control method by encryption.
Group II, claim(s) 43-45, 108-110, drawn to generating the resource key.
Group III, claim(s) 55-63, 120-128, drawn to generating an encryption key .
Group IV, claims 64-65, 129-130, drawn to a method for providing response to peer system request.

The inventions listed as Groups I, II, III and IV do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group I has a special technical feature of publishing the resource key and encryption key, Group II has a special technical feature of generating the resource key by applying hash function, Group III has a special technical feature of generating encryption private key. Group IV has a special technical feature of providing response to the peer system in an encrypting form.