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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 November 2004 (18.11.2004)

PCT

(10) International Publication Number
WO 2004/100440 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number:
PCT/IB2004/001393

(22) International Filing Date: 28 April 2004 (28.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0310411.4 7 May 2003 (07.05.2003) GB

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MURRAY, Bruce** [GB/GB]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(74) Agent: **WILLIAMSON, Paul, L.**; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

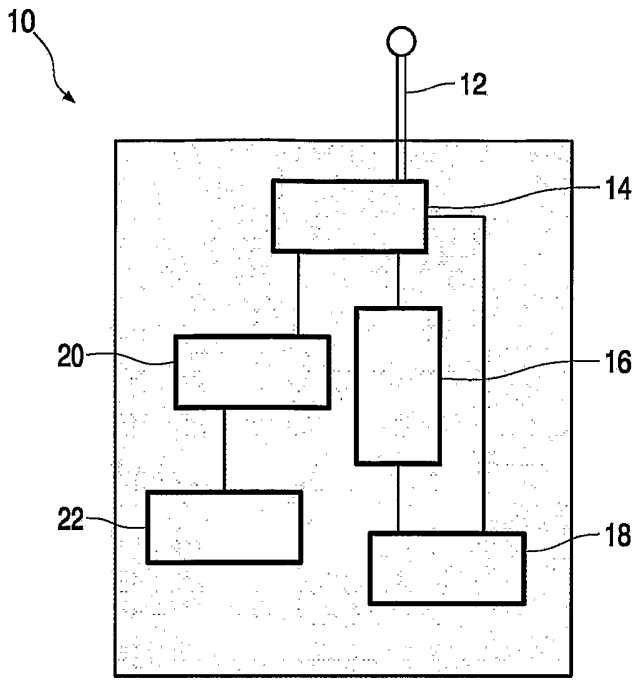
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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,*

[Continued on next page]

(54) Title: ELECTRONIC DEVICE PROVIDED WITH CRYPTOGRAPHIC CIRCUIT AND METHOD OF ESTABLISHING THE SAME



(57) Abstract: The present invention provides for an electronic device having cryptographic computation means arranged to generate cryptographic data within the device for enhancing security of communications therewith, the device including an onboard power supplying means arranged to provide for the driving of the said cryptographic computational means, and so as to provide a device by way of a manufacturing phase and a post manufacturing phase arranged for distribution and/or marketing of the device, and wherein the step of generating the cryptographic data occurs during the post manufacturing phase.

WO 2004/100440 A1

MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *with international search report*

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.

DESCRIPTION

ELECTRONIC DEVICE PROVIDED WITH CRYPTOGRAPHIC CIRCUIT AND METHOD OF ESTABLISHING THE SAME

The present invention relates to an electronic device arranged to exhibit cryptographic security features and to a related method of establishing the same.

In the recent past, an increase in the desire to protect not only the content of communications traffic between entities but also to ensure the correct targeting and retrieval of such information has increased adoption of security features, and in particular such features based on public key cryptography within consumer electronic devices. A common form of such a security arrangement comprise public key cryptographic techniques which allow for an electronic device to prove its identity, and to agree session keys, so as to participate in a secure communication over a particular network thereby allowing secure protection of the content being transmitted from, or received by, the device.

As noted above, in addition to providing protection for the actual content being transmitted, similar approaches to security can be employed in order securely to associate such content with individual devices so as to support "digital rights management" arrangements in which, for example, an audio file can be retrieved and played only on a device belonging to the legitimate purchaser of said file.

A common feature of such a system employing cryptographic techniques is the need to provide the device with a securely embedded public/private key pair. As is known, the private key is generally used to apply a digital signature to outgoing messages, or to decrypt targeted incoming messages or other communication content.

The so-called public key is arranged to be provided to third parties to allow for verification of messages signed by the device, and to allow for the encryption of messages targeted at the device.

In this scenario, there is a significant amount of trust that must be placed with the public key and this is normally achieved by requiring that the public key is digitally signed by an appropriate certification authority. The resulting combination of the public key and signature as provided by the certification authority then forms a device certificate. Such authenticating certificate is readily verifiable by any third party that has been provided with the appropriate public key of the certification authority.

For devices employing a public key arrangement, the device certificate is generally installed within the device at the time of its manufacture and in accordance with either of the two following arrangements.

First, the certification authority creates a public/private keypair, and the certificate associated with the device, on a dedicated computer system, and the appropriate information can then be programmed into the device at a late stage in its manufacture and so prior to its distribution into the relevant market.

As an alternative, the device itself can be arranged to create its own public/private keypair by internal processing during its manufacturing phase, and then subsequently to emit the public key for signing by the certification authority so as to create the device certificate. The device certificate is then again installed in the device at a late stage in its manufacture.

The latter of the two arrangements noted above in which the device creates its own public/private keypair by internal processing offers advantages since a higher level of security can be achieved. As will be appreciated, since the private key of the device can be arranged to be created wholly within the secured hardware domain of the device, it need never be exposed and, as noted, it is only the public key that need be emitted for signature by the certification authority.

However, in arriving at such an advantageously higher degree of security, disadvantages have been identified in that the internal processing required adds significantly to the device serialisation time arising during the manufacturing stage. Also, the internal processing that generates the public/private keypair, particularly in situations in which the RSA public key system is employed, can take in the region of many tens of seconds, or even minutes, especially if the particular device has constrained computational ability in view of it being designed for low power consumption, for example a portable communications device. Potentially problematic delays are then experienced during device production.

Yet further, it is envisaged that many future devices will be arranged to operate within relatively small authorised domains, for example within a particular household, in which the device can associate itself with other devices in close physical proximity during its initial period of use. There is a realization that members of such domains may subsequently become separated geographically, and so require secure communication over public networks.

Within such authorised domains these devices are arranged to operate on a so-called "web-of-trust" principle in which trusted links are allowed only with other devices belonging to that same domain. One commonly known arrangement employing the "web-of-trust" concept is the operating mode of security software known as "PGP".

Within such a "web-of-trust "arrangement, the devices no longer have to employ a hierarchical public key infrastructure, since they need only to have been provided with identifiers and a key pair before the first point of usage within the domain. The generation of a keypair however therefore remains an important consideration even in such arrangements which do not use a classic hierarchical public key infrastructure.

The present invention seeks to provide for an electronic device offering cryptographic security, and a method of establishing the same, and which have advantages over known such systems in which the cryptographic data is to be generated internally within the device.

According to a first aspect of the present invention there is provided an electronic device having cryptographic computation means arranged to generate cryptographic data within the device for enhancing security of communications therewith, the device including an onboard power supplying means arranged to provide for the driving of the said cryptographic computational means.

Through employing an onboard power supplying means, the cryptographic computational means can be arranged advantageously to generate the cryptographic data subsequent to the manufacturing of the device and, in particular, during the phases when the manufactured device might otherwise be laying dormant, i.e. prior to, during and just after packaging, and during transportation and shipment for eventual retail. Employment of an onboard power supply so as to allow for the post-production generation of the cryptographic data therefore advantageously reduces production costs and delays by removing the serialisation step from the manufacturing phase of the device.

Also, since relatively long periods may be available for such processing by the cryptographic computational means so as to generate the cryptographic data, a relatively high standard of security can therefore be achieved.

It will be appreciated that the invention therefore provides, in addition to the technical advantages as compared with the prior-art requirements for serialisation during production, additional advantages in that the cryptographic data and the related serialisation can be selectively initiated only in relation to device that have a higher probability of actually being sold and this can vastly reduce processing steps that might otherwise be wasted on eventually unsold devices.

The features of Claims 2-5 relate to particularly advantageous arrangements in which the power supplying means can be selectively activated as required and can also form part of the principal power supplying means arranged for future normal operation of the device so as to advantageously reduce potential duplication of power supplements within the device.

The features of Claims 6 and 7 are advantageous in ensuring that the maximum advantages can be achieved by the present invention whilst minimising disruption to the manufacturing-retail cycle.

According to another aspect of the present invention there is provided a method of establishing cryptographic data within an electronic device, and comprising the steps of generating cryptographic data within the device for enhancing security of communications therewith, and under power provided by means of an onboard power supplying means.

The feature of Claim 13 is particularly advantageous in allowing for control of the commencement of the internal generation of the cryptographic data and in relationship with the packaging and/or transportation of the device.

According to yet another aspect of the present invention, there is provided a method of providing a device with cryptographic data and including a manufacturing phase and a post manufacturing phase arranged for distribution and/or marketing of the device, and including the step of generating the cryptographic data during the post-manufacturing phase.

The feature of Claim 19 is particularly advantageous in allowing for authentication of a public key subsequent to packaging of the device.

The invention is described further hereinafter, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 is a schematic block diagram of an electronic device embodying the present invention; and

Fig. 2 is a flow diagram illustrating operation of a device such as that in Fig. 1 in accordance with an embodiment of the present invention.

Turning now to Fig. 1, there is illustrated an electronic device in the form of a mobile phone 10 which, in accordance with its normal mode of operation, is required to transmit and receive secure communication signals by way of its antenna 12.

The mobile phone 10 includes standard electronic circuitry and which is not illustrated in detail in the drawing with the exception of a transmitting/receiving section 14, timebase control section 16 and a rechargeable battery 18 for powering normal use of the phone.

In addition, the mobile phone 10 includes a cryptographic generation section 20 arranged for generating public/private keypairs as part of a public key cryptographic arrangement and which, in accordance with the illustrated embodiment of the present invention, is arranged to be powered for such operation by means of a disposal battery 22 which can be readily inserted in, and removed from, the mobile phone 10.

Such insertion of the disposable battery 22 is arranged to initiate operation of the cryptographic generation section 20 as required. However, as an alternative, switch means can be included (not shown) so as to allow for the selected initiation of the cryptographic generation section 20 by means of the disposable battery 22.

The mobile phone 10 as illustrated has been designed from the recognition that, with regard to such devices, the time spent by the product during its packaging, distribution and retailing phases can usefully be employed for cryptographic computation measures so that such measures are then removed from, and therefore simplify and expedite, the manufacturing phase.

Thus, the device 10 can be manufactured and, as illustrated, fitted with a disposable battery 22 and then steps taken to initiate the cryptographic computation within the cryptographic generation section 20 shortly prior to packaging and distribution and without any external device serialisation for cryptographic purposes.

As an alternative, the disposable battery 22 can be omitted and predetermined amount of charge provided to the rechargeable battery 18 of the mobile phone 10, which predetermined amount of charge is sufficient to drive the cryptographic computation within the section 20 during the device's post-production phase. Production costs and related delays are therefore advantageously removed by means of the aforementioned serialisation steps.

Dependent upon the marketing/transport route taken by the device, days, or even possibly weeks, will be available for the product to perform its own keypair generation internally within the cryptographic generation section 20. The product design and key generation algorithms are of course advantageously selected so as to ensure that such cryptographic computation processors will be completed by the time the product is made available to the end customer.

An associated advantage arises here in that, in allowing for relatively long processing periods, i.e. at least days instead of minutes as currently available, the cryptographic processes can be performed to a higher standard of security than would be economically viable were such processes to be executed during the latter stages of the production phase as currently occurs.

Yet further, it becomes advantageously possible to control the frequency of operation of the processing elements of the cryptographic generation section 20 so as to ensure only low power consumption, and thus low heat dissipation and radiation etc. once the product has been packaged and during its transit to, for example, its retail location.

Turning now to Fig. 2, there is provided a block flow diagram illustrating a method according to an embodiment of the present invention.

The method commences at a block 24 with the actual manufacture of the device, for example a mobile telephone 10 of Fig. 1, and then proceeds into a post-manufacturing phase at block 26 at which the cryptographic computation is activated by means of the disposable battery 22 so as to generate internally within the device, a public/private keypair at block 26.

Subsequent to initiation of the cryptographic processing, and while such processing is ongoing, the device is packaged at block 28 and subsequently transported at block 30 to its retail location identified by block 32.

In accordance with the embodiment illustrated by reference to Fig. 2, the mobile phone 10 exhibits a requirement for operation that requires its public key to be signed into a digital certificate by a certification authority and this is illustrated at block 34. This step in the process can be provided at the point of sale of the mobile phone 10.

Such a feature serves to illustrate a particular further advantage of the present invention in that, in addition to the technical advantages arising as compared with the serialisation as currently occurring during production and as noted above, commercial and economic advantages arise in that the serialisation now occurring in accordance with the present invention need only occur shortly prior to the actual sale of the device. This ensures that device serialisation effort is not then wasted on unsold devices.

In accordance with another embodiment of the present invention, if the product concerned is to be used wholly with an authorized domain, it can then be arranged to conduct whatever "web-of-trust" associations are needed during its initial period of operation shortly after retailing, for example after being unpacked by the end customer. In this scenario, the certification block 34 illustrated in Fig. 2 is replaced by a mere "initial use" block.

As will therefore be appreciated from the above, the present invention is advantageous in reducing production costs and production times, of portable devices by removing the need to conduct cryptographic serialisation at a late stage in the production phase of the device. The time spent by the product in its distribution and retailing phases is advantageously utilised by allowing the device to perform internal cryptographic keypair generation whilst packaged.

As discussed above, the device can then be put into service immediately by an end customer subsequent to purchase if it is to be used in a "web-of-trust" authorised domain. However, if operation device requires a digital certificate issued by a digital certification authority, then the certificate can be create and installed in the device at the point of sale.

The invention is not restricted to the details of the foregoing embodiments. For example, it should be appreciated that the device and method of the present invention can be incorporated within any appropriate device, and in particular a mobile device requiring security of communication and/or connectivity.

Also, reference to communication is not restricted to electronic communication. For example, one might have a portable disc player device that generates its own keypair according to the invention, has its public key read and registered at a trustworthy point of sale such that no certificate is created or installed. The user can then receives packaged media, such as CD-R discs, through the postal system or other physical form of transport and delivery.

CLAIMS

1. An electronic device having cryptographic computation means arranged to generate cryptographic data within the device for enhancing security of communications therewith, the device including an onboard power supplying means arranged to provide for the driving of the said cryptographic computational means.

2. A device as claimed in Claim 1 wherein the onboard power supplying means comprises a selectively activated power supply means.

3. A device as claimed in Claim 1 or 2, wherein the power supply means comprises a battery.

4. A device as claimed in Claim 1, 2 or 3, wherein the power supply means comprises a disposable temporary power supply means.

5. A device as claimed in Claim 1, 2 or 3, wherein the power supply means comprises an at least part charge rechargeable power supply means.

6. A device as claimed in any one or more of Claims 1-5 wherein the cryptographic computation means is arranged to be activated so that cryptographic computation can operate after the device has been packaged for distribution and retail purposes.

7. A device as claimed in Claim 6, wherein the cryptographic computation means is arranged to operate during transportation of the device.

8. A device as claimed in any one or more of Claims 1-7, wherein the cryptographic computation means is arranged to generate cryptographic keys.

9. A device as claimed in Claim 8, wherein the cryptographic computation means is arranged to generate a public/private keypair.

10. A device as claimed in Claim 9, and arranged such that the public key can be made available for certification purposes.

11. A device as claimed in Claim 9, and arranged for operation within an authorised domain.

12. A method of establishing cryptographic data within a mobile device, and comprising the steps of generating cryptographic data within the device for enhancing security of communications therewith, and under power provided by means of an onboard power supplying means.

13. A method as claimed in Claim 12 and including the step of selectively activating the generation of the cryptographic data by control of the onboard power supplying means.

14. A method as claimed in Claim 12 or 13, wherein the cryptographic data comprises cryptographic key information.

15. A method as claimed in Claim 14, wherein the cryptographic key information, is a public/private keypair.

16. A method as claimed in Claim 15, and including the step of making the public key available for certification purposes.

17. A method as claimed in any one or more of Claims 12-16, and in which the steps are taken during a post manufacturing phase of the device.

18. A method of providing a device with cryptographic data and including a manufacturing phase and a post manufacturing phase arranged for

distribution and/or marketing of the device, and including the step of generating the cryptographic data during the post manufacturing phase.

19. A method as claimed in Claim 18, and including the step of creating a device certificate for the device subsequent to packaging of the device.

20. A method as claimed in Claim 19, and including the step of creating the device certificate at a point of sale of the device.

1/1

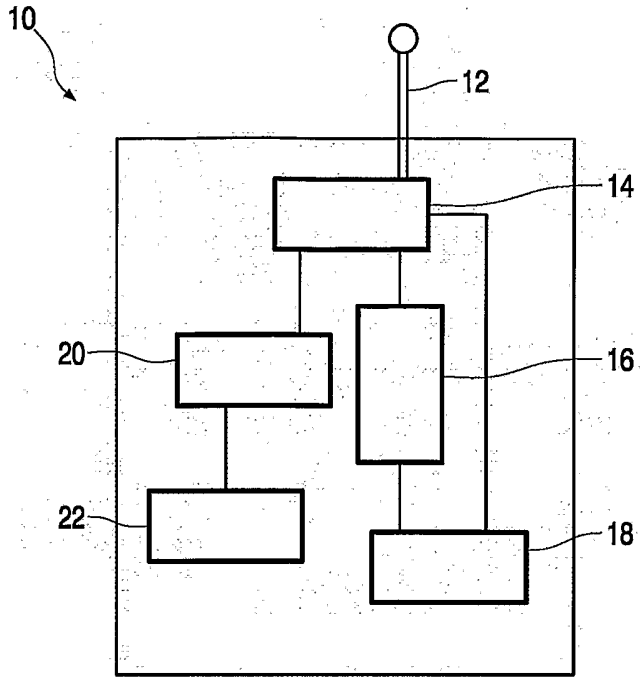


FIG.1

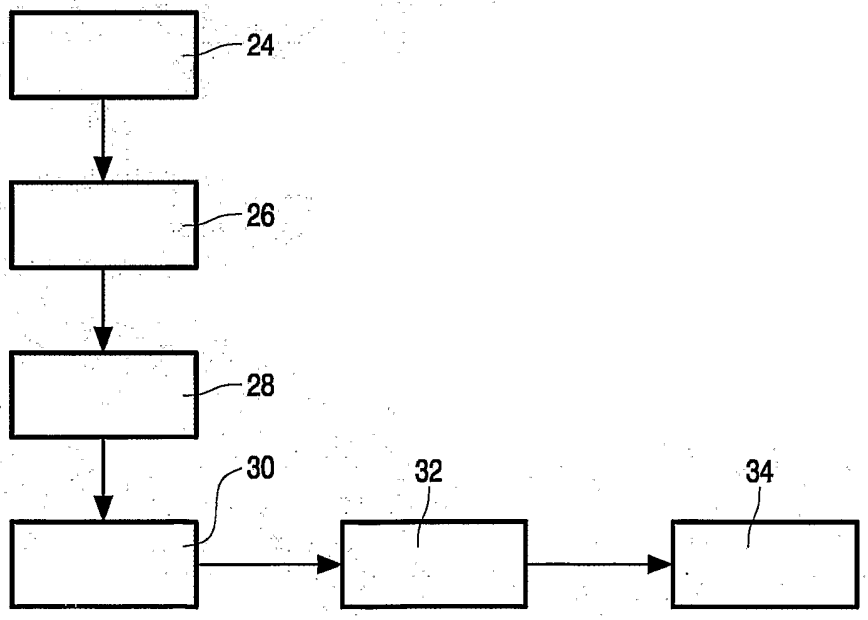


FIG.2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/001393

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

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)
IPC 7 H04L

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, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/021419 A1 (HANSEN MADS DORE ET AL) 30 January 2003 (2003-01-30) abstract page 2, paragraph 10 page 2, left-hand column, line 58 - right-hand column, line 5 page 3, right-hand column, line 32 - line 36 page 4, paragraph 35 - paragraph 36; figure 3	1,3,5,6, 8,9,12, 14,15
X	EP 0 533 507 A (MAS HAMILTON GROUP) 24 March 1993 (1993-03-24) column 1, line 58 - column 2, line 27 column 12, line 8 - line 13; figure 4 claim 1	1,3,6,8

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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
28 July 2004	05/08/2004

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, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dujardin, C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/001393

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/116342 A1 (KAWAHARA TAKAYUKI ET AL) 22 August 2002 (2002-08-22) page 2, left-hand column, line 15 - line 21 page 5, right-hand column, line 9 - line 15; figures 3A,3B,4A,4B	1,6-8,18
X	EP 1 081 891 A (COMPAQ COMPUTER CORP) 7 March 2001 (2001-03-07) abstract paragraph '0014! - paragraph '0018!	18,19
X	US 6 115 816 A (DAVIS DEREK L) 5 September 2000 (2000-09-05) column 5, line 13 - line 44; figure 4	18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2004/001393

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003021419 A1	30-01-2003	EP 1421548 A1	26-05-2004
		SE 0102474 A	12-01-2003
		WO 03007228 A1	23-01-2003
EP 0533507 A	24-03-1993	US 5170431 A	08-12-1992
		CA 2078652 A1	21-03-1993
		EP 0533507 A1	24-03-1993
		JP 7189537 A	28-07-1995
US 2002116342 A1	22-08-2002	JP 2002245235 A	30-08-2002
EP 1081891 A	07-03-2001	EP 1081891 A2	07-03-2001
		JP 2001148697 A	29-05-2001
		TW 560158 B	01-11-2003
US 6115816 A	05-09-2000	US 5818939 A	06-10-1998
		AU 5956598 A	15-07-1998
		DE 19782199 T0	18-11-1999
		GB 2336080 A ,B	06-10-1999
		WO 9827685 A1	25-06-1998