

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 November 2003 (13.11.2003)

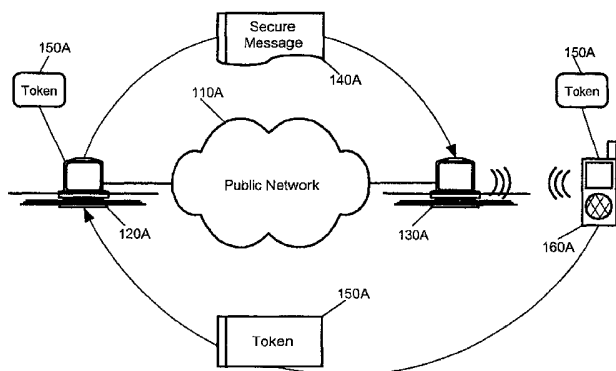
PCT

(10) International Publication Number
WO 03/094476 A1

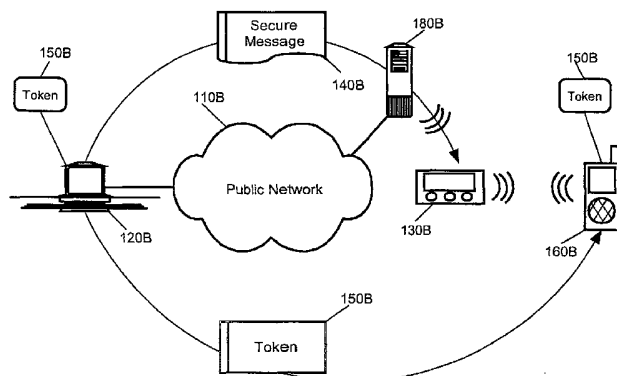
- (51) International Patent Classification⁷: **H04L 29/06** (72) Inventors: **BARRUS, William**; 107 Murdock Creek Court, Apex, NC 27502 (US). **BATES, Cary**; 450 73rd Street NW, Rochester, MN 55901 (US). **CRENSHAW, Robert**; 111 Ferncroft Court, Apex, NC 27502 (US). **DAY, Paul**; 1428 12th Avenue NE, Rochester, MN 55906 (US).
- (21) International Application Number: PCT/GB03/01344
- (22) International Filing Date: 27 March 2003 (27.03.2003)
- (25) Filing Language: English (74) Agent: **LITHERLAND, David, Peter**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).
- (26) Publication Language: English
- (30) Priority Data: 10/134,184 29 April 2002 (29.04.2002) 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
- (71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).
- (71) Applicant (*for MG only*): **IBM UNITED KINGDOM LIMITED** [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB). (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: ENHANCED MESSAGE SECURITY



A



B

(57) Abstract: A secure messaging method includes the steps of receiving an encrypted message, the message having been encrypted using a token of a corresponding pervasive device; wirelessly verifying the presence of the pervasive device; and, if the presence can be verified, decrypting the message using the token. The verification step can include the steps of establishing a wireless link with the pervasive device; and, querying the pervasive device over the wireless link. In particular, the establishing step can include the step of establishing a Bluetooth link with the pervasive device. Furthermore, the querying step can include the step of requesting geographic coordinates which locate the pervasive device.

WO 03/094476 A1



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, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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.

Published:

— *with international search report*

ENHANCED MESSAGE SECURITY**Technical Field of the Invention**

5 The present invention relates to message security and more particularly to securing electronic messages through wireless device based authentication.

Background of the Invention

10 Electronic messaging, and in particular, the use of electronic mail (e-mail) and instant messengers (IM), continues to grow at an astounding rate. In consequence, it appears that electronic messaging, including e-mail and IM, has become a critical mode of interpersonal communications
15 rivalled only by wireless communications. Nevertheless, every transmitted message can result in an unintentional breach of security. In particular, when a party other than the intended recipient of the message accesses the message, the intent of a secure transaction will have been lost.

20 Technologies have been implemented in recent years to remediate some of the actual and perceived risks associated with electronic messaging. In particular, asymmetrical encryption algorithms have been applied to ensure not only that only a key-bearing recipient can access encrypted content, but also that only the intended recipient who bears the key can
25 access the encrypted content. Still, as has become well-known in the field of short and long-range wireless communications, wireless transmissions are inherently susceptible to unauthorized capturing by third party receivers.

30 In particular, line-of-sight communications protocols have always been susceptible both to intentional and inadvertent breaches of communications security. Similarly, both proposed and maturing short-range wireless technologies such as Bluetooth, Wi-Fi and other IEEE 802.11 variants, are vulnerable to the capturing of sensitive data by
35 unauthorized users. Wi-Fi technologies in particular have become a cause for concern in the corporate environment and, in consequence, a feverish pace of urgent development has produced several technological stop-gap measures which directly address security in Wi-Fi networks. Still, no one stop-gap measure has proven to be an effective measure for secured
40 messaging.

Notwithstanding the security risks of wireless messaging, the proliferation of wireless, pervasive devices as a means for interpersonal communications is unprecedented. Many advantages associated with the use of wireless, pervasive devices in computing applications remain wholly
5 absent from conventional computing. For instance, whereas fixed location computing ordinarily associated with the conventional computing in itself provides no added dimension, wireless, pervasive computing adds a personal dimension to computing.

Specifically, wireless, pervasive computing devices like cellular
10 telephones and personal digital assistants are seldom associated with a fixed location. Rather, wireless, pervasive computing devices, more often than not, are closely associated with the locale of the user. Still, few emerging technologies appreciate the personal dimension of wireless,
15 pervasive computing. More importantly, no emerging technologies capitalize upon the personal dimension of wireless, pervasive computing in the context of secure messaging.

Summary of the Invention

20 The present invention provides a secured messaging system and method. A secure messaging system includes a message source and a message recipient, communicatively linked to one another through a computer communications network. The system also includes a pervasive computing
25 device and at least one token which uniquely identifies the pervasive computing device. The system further includes a first wireless communications receiver/transmitter disposed in the message recipient, and a second wireless communications receiver/transmitter disposed in the pervasive computing device.

30 The system includes both an encryption engine associated with the message source, and a decryption engine associated with the message recipient. In particular, the encryption engine is configured to encrypt messages intended for the message recipient with the token. The
35 decryption engine is configured to decrypt the messages with the token only when a wireless link has been established between the first and second wireless receiver/transmitters.

40 In one embodiment of the invention, the first and second wireless receiver/transmitters are short range radio frequency receiver/transmitters. For example, the short range radio frequency receiver/transmitters can comport with the Bluetooth wireless protocol.

Also, the token can include a media access control (MAC) address which corresponds to the pervasive computing device. In one alternative embodiment, a geographic positioning system can be disposed in the pervasive computing device. In that alternative aspect, the token can include a set of geographic coordinates specifying a geographic position for the pervasive device.

A secure messaging method includes the steps of receiving an encrypted message, the message having been encrypted using a token of a corresponding pervasive device; wirelessly verifying the presence of the pervasive device; and, if the presence is verified, decrypting the message using the token. The verification step can include the steps of establishing a wireless link with the pervasive device; and, querying the pervasive device over the wireless link. In particular, the establishing step can include the step of establishing a Bluetooth link with the pervasive device.

The querying step can include the step of sending a request to the pervasive device. Specifically, the request can include one of a request for the token, a request for an decryption key based upon the token, and a request for an acknowledgment of the request. In another aspect of the inventive method, the querying step can include the step of requesting geographic coordinates which locate the pervasive device.

Brief Description of the Drawings

A preferred embodiment of the invention will next be described, by way of example only, with reference to the accompanying drawings.

Figure 1A is a schematic illustration of a secure messaging system in which messages are received and processed in a conventional computing device;

Figure 1B is a schematic illustration of a secure messaging system in which messages are received and processed in a pervasive computing device; and,

Figure 2 is a block illustration of a process for securely communicating messages in the secure messaging system of the present invention.

Detailed Description of the Preferred Embodiments

Figure 1A is a schematic illustration of a secure messaging system in accordance with an embodiment of the invention in which messages are received and processed in a conventional computing device. The system can include two 'conventional' computing devices 120A, 130A configured for data communications through a public network 110A, for example the Internet. The conventional computing devices 120A, 130A can include desktop type computers, server computers, portable laptop computers, mid-range computers, mainframe computers, though the invention is not limited strictly to those computing device types enumerated herein.

Importantly, the conventional computing device 130A is further configured for short range wireless communications, including infrared communications and short range radio frequency communications. Examples of short range radio frequency communications include Wi-Fi™ (IEEE 802.11(b)) and other 802.11 variants, as well as Bluetooth communications and other 802.15 variants, though the invention is not limited to any particular short range radio frequency communications technology. In any case, the conventional computing device 130A can establish and maintain a data communications link over the short range wireless communications channel with the pervasive computing device 160A.

The pervasive computing device 160A can be any such device having a personal dimension, including, for example, a notebook computer, a data ready cellular telephone, a personal digital assistant (PDA), a pager, or an embedded system in a vehicle or article of clothing. Significantly, the pervasive computing device 160A has associated therewith a token 150A. The token 150A is any identifier suitable for definitively identifying the pervasive computing device 160A. One example of a suitable identifier can include a MAC address or other such hardware serial number. The token 150A can be forwarded to the conventional computing device 120A. Subsequently, when a message is to be sent over the public network 110A to the conventional computing device 130A, the message can first be uniquely secured using the token 150A.

In that regard, both symmetric and asymmetric encryption techniques are well-known in the art and, in consequence, the message can be secured with such techniques using the token 150A as an encryption key or as the seed for generating an encryption/decryption key pair. As a result, the secure message 140A can be forwarded to the conventional computing device 130A without fear of an authorized recipient accessing the secured message

140A. Once received, the conventional computing device 130A establishes a wireless link with the pervasive device 160A. Only when the wireless link has been effectively established between the pervasive computing device 160A and the conventional computing device 130A can a token 150A be exchanged between the two.

Once exchanged, the token 150A can be used to formulate the decryption key necessary to decrypt the secured message 140A. Alternatively, where the token 150A is the decryption key, no formulation will be required. In any event, in view of the personal dimension of the pervasive computing device 160A, the proximity of the pervasive computing device 160A to the conventional computing device 130A can be used to increase the probability that the recipient of the secured message is the intended recipient. Moreover, where only the token 150A and not the encryption key has been wirelessly communicated between the conventional computing device 130A and the pervasive computing device 160A, the insecurities associated with short range wireless communications can be circumvented.

Importantly, while in Figure 1A, the conventional computing devices 120A, 130A are shown to be computers likely associated with a fixed location, the conventional computing devices 120A, 130A can include other pervasive computing devices such as a PDA, data enabled cellular telephone, paging device, or other such embedded system. In that regard, Figure 1B is a schematic illustration of a secure messaging system in which messages forwarded by a conventional computing device are received and processed in a pervasive computing device.

The system of Figure 1B can include a conventional computing device 120B and a first pervasive computing device 130B, both configured for data communications through a public network 110B, for example the Internet, via a wireless gateway 180B configured to support communications with the first pervasive computing device 130B. As in the case of Figure 1A, in the system of Figure 1B, the first pervasive computing device 130B can be further configured for short range wireless communications, including infrared communications and short range radio frequency communications. Using a short range wireless communications channel, the first pervasive computing device 130B can establish and maintain a data communications link with a second pervasive computing device 160B.

The second pervasive computing device 160B can have associated therewith a token 150B. As before, the token 150B can be any identifier

suitable for definitively identifying the second pervasive computing device 160B, including, for example, a MAC address or other such hardware serial number. Prior to engaging in secure communications between the conventional computing device 120B and the first pervasive computing device 130B, the token 150B can be forwarded to the conventional computing device 120B. Subsequently, when a message is to be sent over the public network 110B to the first pervasive computing device 130B, the message first can be uniquely secured using the token 150B.

In particular, the message can be secured with such techniques using the token 150B as an encryption key or as the seed for generating an encryption key. As a result, the secured message 140B can be forwarded to the first pervasive computing device 130B without fear of an authorized recipient accessing the secured message 140B. Once received, the first pervasive computing device 130B can establish a wireless link with the second pervasive computing device 160B. Only when the wireless link has been effectively established between both pervasive computing devices 130B, 160B can a token 150B be exchanged between the two. Once exchanged, the token 150B can be used to formulate the decryption key necessary to decrypt the secured message 140B. Alternatively, where the token 150B is the decryption key, no formulation will be required.

In any event, in view of the personal dimension of the second pervasive computing device 160B, the proximity of the second pervasive computing device 160B to the first pervasive computing device 130B can be used to increase the probability that the recipient of the secured message is the intended recipient. Moreover, where only the token 150B and not the encryption key has been wireless communicated between the pervasive computing devices 130B, 160B, the insecurities associated with short range wireless communications can be circumvented.

Figure 2 is a block illustration of a process for securely communicating messages in the secure messaging system of a preferred embodiment of the present invention. A message source 210 can securely exchange messages 200 in encrypted form 250 with a message recipient 220. In particular, the messages 200 can be placed in encrypted form 250 using an encryption key based upon a token 240. The token 240 can be any suitable identifier which uniquely identifies a pervasive computing device 230 personally associated with the message recipient 220. Though many such identifiers are contemplated, examples can include the MAC address of the pervasive computing device 230, or even the geographic position of the pervasive computing device 230. Notably, the token 240 can be acquired by

the message source 210 both directly from the pervasive computing device 230, or indirectly through a peer- to-peer indexing scheme, or through a centralized registry.

5 Once in encrypted form 250, the message 200 can be forwarded to the recipient. Advantageously, the recipient's identity can be ensured by requiring the presence of the pervasive computing device 230 when
10 decrypting the message 200 in its encrypted form 250. In particular, the presence of the pervasive computing device 230 can be confirmed using
15 several techniques. In one preferred embodiment, the decryption key which can be formulated based upon the token 240 can be forwarded to the
 pervasive computing device 230 by the message source 210. When the message recipient 220 attempts to access the message 200 in its encrypted
 form 250, the message client in the message recipient can query the
 pervasive computing device 230 for the decryption key.

 Notwithstanding, other configurations are equally preferred. For instance, in an alternative preferred embodiment, the encryption key which
20 had been formulated based upon the token 240 can be pre-stored in the pervasive computing device 230. In another alternative preferred
 embodiment, a notification can be forwarded to the pervasive computing device 230 in response to the receipt by the message recipient 220 of the
 encrypted form 250 of the message 200. The notification can request that the pervasive computing device 230 establish a communicative link with the
25 message source 210 in order to retrieve the decryption key.

 In yet another alternative embodiment, the encryption key can be forwarded with the encrypted form 250 of the message 200 to the message
30 recipient 220. Upon receipt, the message recipient 220 can query the pervasive computing device 230 for the token. Moreover, as it is known
 that in some short range communications protocols, device identifiers can be transmitted as a matter of course in communications, in some short
 range communications protocols when combined with the present invention, merely a proceed or not to proceed query and query response can be
35 exchanged between the message recipient 220 and the pervasive computing device 230.

 Notably, aside from hardware identifiers, the token 240 can include the geographic position of the pervasive computing device 230. In that
40 regard, the message 200 can be placed in encrypted form 250 according to a proposed geographic position of the pervasive computing device 230. Where
 the actual geographic position of the pervasive computing device 230

compares favorably to the proposed geographic position upon receipt of the message 200 in its encrypted form 250, the decryption key required to access the message 200 can be computed based upon the geographic position of the pervasive computing device 230.

5

In view of the personal dimension of the pervasive computing device which, as described herein, typically will be required to access secure messages exchanged between a message source and message recipient, it will be recognized that communicative difficulties can arise where the
10 pervasive computing device has been damaged, discarded, misplaced, lost or stolen by the message recipient. To circumvent such infrequent circumstances, in accordance with the present invention, the message recipient can establish an auxiliary communicative link with the message source in order to receive the decryption key upon establishing the
15 identity of the message recipient to the satisfaction of the message source.

Thus has been described a secure messaging system in which messages are secured using a token linked to a pervasive computing device
20 personally associated with the intended recipient. The secured message is forwarded through conventional data communications channels to the intended recipient. Upon receipt, the receiving computing device of the intended recipient retrieves the token from the pervasive device in order to access the secured message. In particular, the receiving computing
25 device establishes a wireless communicative link with the pervasive device through which link the token can be communicated to the recipient.

The present invention can be implemented as a computer performed process within hardware, software or a combination of hardware and
30 software. An implementation of the method and system of the present invention can be realized in a centralized fashion in one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system, or other apparatus adapted for carrying out the methods described herein, is
35 suited to perform the functions described herein.

A typical combination of hardware and software could be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the
40 methods described herein. The present invention can also be embedded in a computer program product, which comprises all the features enabling the

implementation of the methods described herein, and which, when loaded in a computer system is able to carry out these methods.

Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following a) conversion to another language, code or notation; b) reproduction in a different material form.

CLAIMS

1. A secure messaging system, comprising:

5 a message source and a message recipient, communicatively linked to one another through a computer communications network;

a pervasive computing device; at least one token which uniquely identifies said pervasive computing device;

10 a first wireless communications receiver/transmitter disposed in said message recipient, and a second wireless communications receiver/transmitter disposed in said pervasive computing device;

15 an encryption engine associated with said message source configured to encrypt messages intended for said message recipient with said at least one token; and,

20 a decryption engine associated with said message recipient configured to decrypt said messages with said at least one token only when a wireless link has been established between said first and second wireless receiver/transmitters.

25 2. The secure messaging system of claim 1, wherein said first and second wireless receiver/transmitters are short range radio frequency receiver/transmitters.

30 3. The secure messaging system of claim 2, wherein said short range radio frequency receiver/transmitters comport with the Bluetooth wireless protocol.

35 4. The secure messaging system of any preceding claim, wherein said token comprises a media access control (MAC) address which corresponds to said pervasive computing device.

5. The secure messaging system of any preceding claim, further comprising a geographic positioning system disposed in said pervasive computing device.

40 6. The secure messaging system of claim 5, wherein said token comprises a set of geographic coordinates specifying a geographic position for said pervasive device.

7. A secure messaging method, the method comprising the steps of:

receiving an encrypted message, said message having been encrypted
using a token of a corresponding pervasive device;

wirelessly verifying the presence of said pervasive device; and,

if said presence can be verified, decrypting said message using said
token.

8. The secure messaging method of claim 7, wherein said verification
step comprises the steps of:

establishing a wireless link with said pervasive device; and,

querying said pervasive device over said wireless link.

9. The secure messaging method of claim 8, wherein said establishing
step comprises the step of establishing a Bluetooth link with said
pervasive device.

10. The secure messaging method of claim 7, wherein said querying step
comprises the step of sending a request to said pervasive device, said
request comprising one of a request for said token, a request for an
decryption key based upon said token, and a request for an acknowledgment
of said request.

11. The secure messaging method of claim 7, wherein said querying step
comprises the step of requesting geographic coordinates which locate said
pervasive device.

12. A machine readable storage having stored thereon a computer program
for secured messaging, said computer program comprising a routine set of
instructions for causing the machine to perform the steps of any of claims
7 to 11.

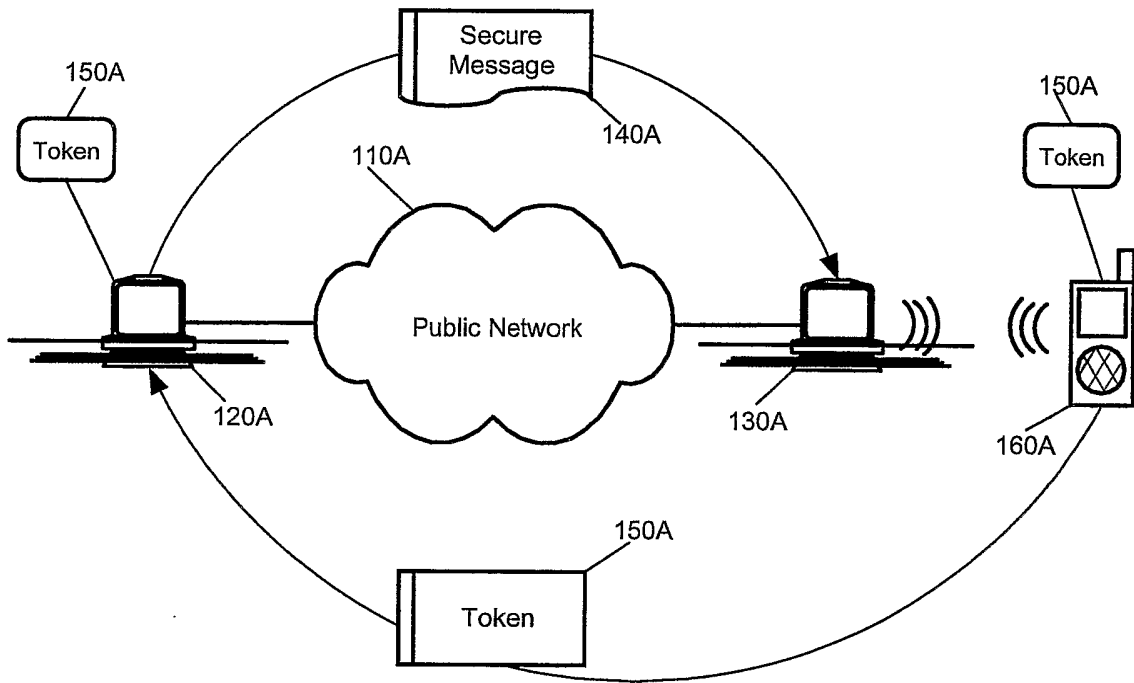


FIG.1A

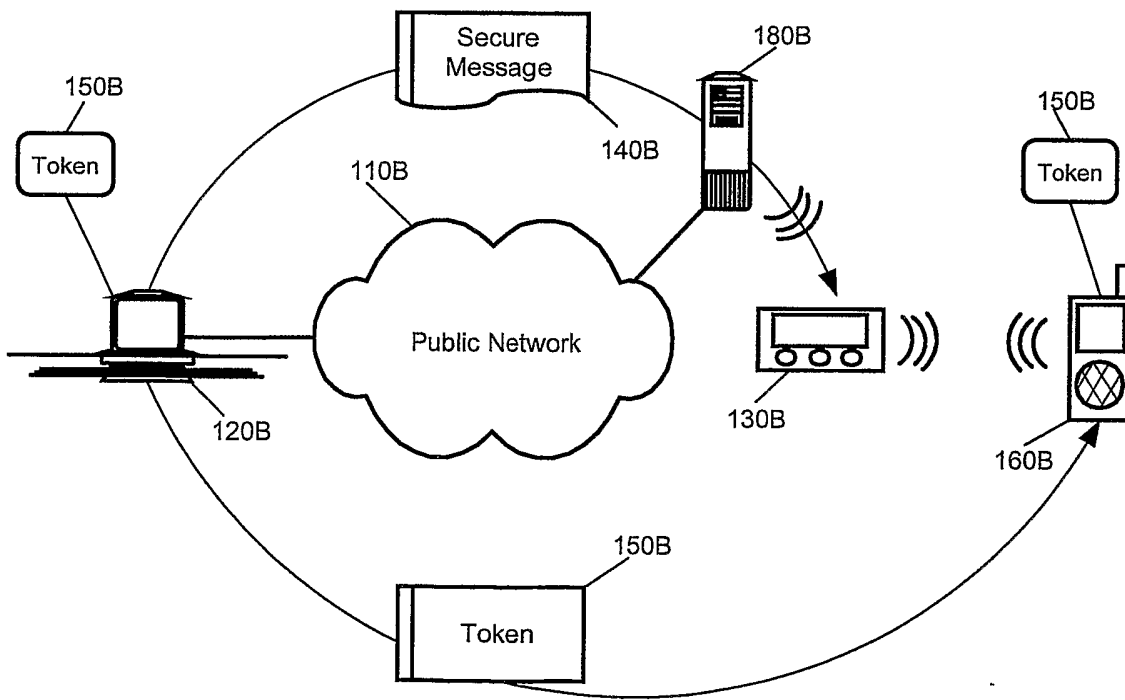


FIG.1B

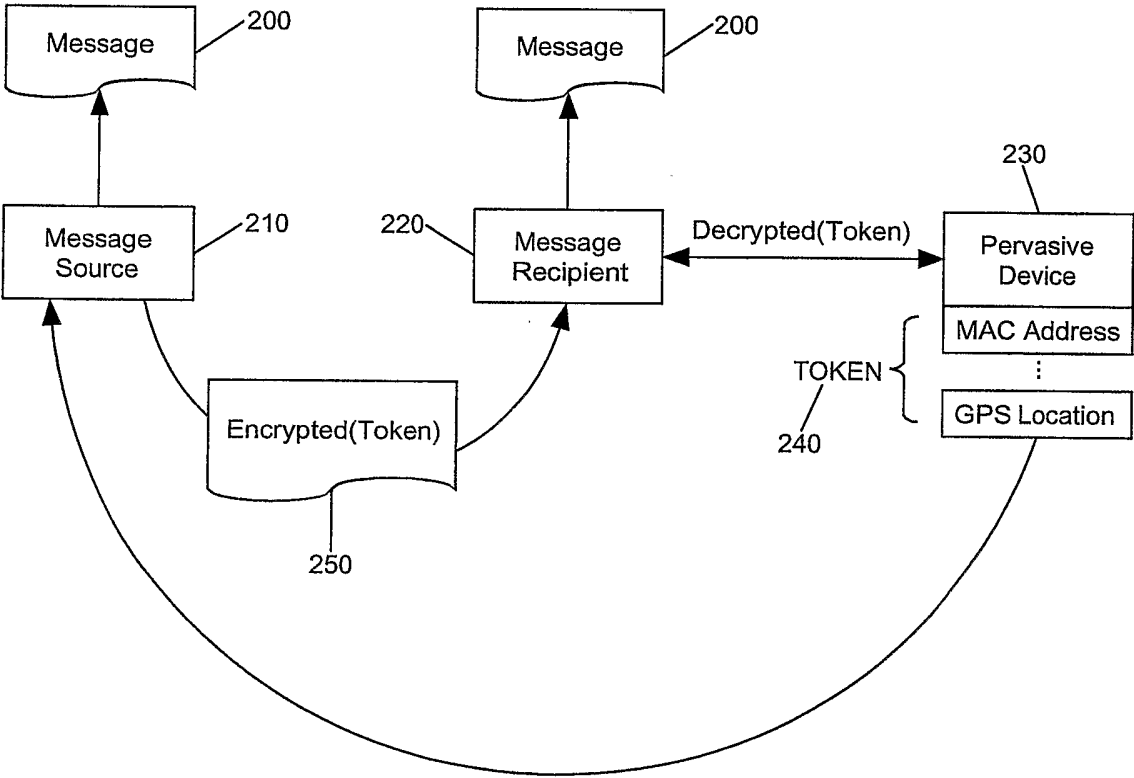


FIG. 2

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/GB 03/01344

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

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 H04Q

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, INSPEC, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 146 692 A (NOKIA CORP) 17 October 2001 (2001-10-17) paragraph '0020! - paragraph '0022! paragraph '0036! - paragraph '0044! paragraph '0047! - paragraph '0049! claim 1 -----	1-12
A	EP 0 989 712 A (PHONE COM INC) 29 March 2000 (2000-03-29) paragraph '0014! - paragraph '0020! claim 7 -----	1-12
A	US 5 878 142 A (AMORUSO VICTOR P ET AL) 2 March 1999 (1999-03-02) abstract column 2, line 20 - line 54 claim 1 -----	1-12



Further documents are listed in the continuation of box C.



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

31 July 2003

Date of mailing of the international search report

08/08/2003

Name and mailing address of the ISA

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

Authorized officer

Raposo Pires, J

INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/GB 03/01344

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1146692	A	17-10-2001	EP 1146692 A2	17-10-2001
EP 0989712	A	29-03-2000	US 6317831 B1	13-11-2001
			CN 1249586 A	05-04-2000
			EP 0989712 A2	29-03-2000
			JP 2000138665 A	16-05-2000
			KR 2000028706 A	25-05-2000
US 5878142	A	02-03-1999	US 5546463 A	13-08-1996
			US 5778071 A	07-07-1998