

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

---

*Ex parte* AMIT GUPTA and PAUL W. JARDETZKY

---

Appeal No. 2002-1527  
Application No. 08/885,817

---

ON BRIEF

---

Before FLEMING, DIXON, and BARRY, *Administrative Patent Judges*.  
BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

A patent examiner rejected claims 1-35. The appellants appeal therefrom under 35 U.S.C. § 134(a). We affirm-in-part.

BACKGROUND

The invention at issue on appeal relates to "multicasting" via the Internet. Multicasting comprises one-to-many and many-to-many communications wherein at least one source sends to data to more than one receiver. For example, multicasting is used to transmit corporate messages to employees and to transmit stock quotes to brokers. (Spec. at 1.) The "IP multicast" protocol supports such transmissions via a

simple design: a sender sends data to a multicast group address, and a network sends the data to everyone who expressed interest in receiving data via that address. (*Id.* at 1-2.)

The appellants explain that when using IP multicast, however, "everyone can listen to a multicast session and everyone can send data to multicast sessions." (*Id.* at 3.) Because anyone can send data to a multicast session, they add, "the potential for disruption by an interloper is significant." (*Id.*)

Accordingly, the appellants expand multicasting to include "private multicasts." (*Id.* at 32.) More specifically, an address space dedicated to multicasting is partitioned into a subspace for public multicasts and a subspace for private multicasts. A public key/private key encryption pair is used for the private multicasts. (*Id.*) The public key is installed on a domain name server or on a certification authority. A user desiring to join a private multicast must apply with a multicast join request, which includes data encrypted using the private key. (*Id.* at 4.) Upon receipt of the request, a router retrieves the associated public key. Using the public key, the router decrypts the encrypted portion of the request to determine if the requestor is authorized to join the private multicast. "Group specific multicast joins are also permitted by sending a bit-

mask identifying a group of senders . . . authorized or prohibited from sending to a user joining a multicast." (*Id.* at 32.)

A further understanding of the invention can be achieved by reading the following claim.

1. A routing element for multicast digital communications, comprising:
  - a. at least one input port;
  - b. at least one output port; and
  - c. a processor for controlling packet routing from an input port to an output port, said processor configured to obtain a public key and to decode at least a portion of a multicast join request comprising encrypted information submitted by a user using said public key to verify that said user is authorized to join a multicast.

Claims 1, 4, 5, 7, 8, 14, 17-19, 22-24, 26, 28, and 32 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,668,877 ("Aziz"). Claims 2, 3, 11-13, 15, 16, 25, 27, 29, and 33-35 stand rejected under 35 U.S.C. § 103(a) as obvious over Aziz. Claims 6, 10, 21, 30, and 31 stand rejected under § 103(a) as obvious over Aziz and U.S. Patent No. 5,237,565 ("Henrion"). Claims 9, 20, 27, 29, 33, and 35 stand rejected under § 103(a) as obvious over Aziz and U.S. Patent No. 5,754,938 ("Herz").<sup>1</sup>

---

<sup>1</sup>The examiner explains that "claims [21 and 30] were erroneously included in the list of claims in the heading of the 35 USC 103 rejection combining *Aziz* and *Herz*." (Supp. Examiner's Answer at 22.) Because claim 31 depends from claim 30, we conclude that inclusion of the dependent claim in the examiner's statement of the

## OPINION

Our opinion addresses the rejections in the following order:

- claims 1 and 3
- claims 2, 11, 15, 25, 34, and 35
- claim 4
- claim 5
- claims 6, 21, 30, and 31
- claims 7-10, 19, 20, 28, and 29
- claim 12
- claim 13
- claims 14, 17, 22, 32, and 33
- claim 16
- claims 18, 26, and 27
- claims 23 and 24.

### A. CLAIMS 1 AND 3

Rather than reiterate the positions of the examiner or the appellants *in toto*, we address the points of contention therebetween. Observing that "Aziz discloses that encrypting and decrypting nodes I (the sender) and J (the receiver) can be firewalls leading into private networks 22 and 30 (Fig. 2 . . . and col. 6, line 58 - col 7, line 9) and that node J delivers the packet 'to an appropriate local transport entity, or other outbound interface' (col 11, lines 9-13)," (Supp. Examiner's Answer<sup>2</sup> at 12), the

---

rejection over Aziz and Herz, (*id.* at 9), was also in error. Therefore, we omit claim 31 from our statement of the rejection.

<sup>2</sup>We rely on and refer to the supplemental examiner's answer, (Paper No. 21), which "replaces the previous Examiner's Answer of December 17, 2001, in which the Examiner inadvertently omitted responses to the Appellant's arguments pertaining to [c]laims 14-16." (Supp. Examiner's Answer at 1.) The original examiner's answer was

examiner finds "the nodes are routing the join requests from a computer within one private network to a computer in another private network. . . ." The appellants argue, "[t]he Aziz multicast protocol described in the reference does not involve action at any routers." (Supp. Appeal Br.<sup>3</sup> at 6.)

In addressing the point of contention, the Board conducts a two-step analysis. First, we construe the claim in question to determine its scope. Second, we determine whether the construed claim is anticipated.

#### 1. Claim Construction

"Analysis begins with a key legal question -- *what is the invention claimed?*" *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1567, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987). In answering the question, "the Board must give claims their broadest reasonable construction. . . ." *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1668 (Fed. Cir. 2000).

---

not considered in deciding this appeal.

<sup>3</sup>We rely on and refer to the supplemental appeal brief, (Paper No. 21), in lieu of the original appeal brief, (Paper No. 16), because the latter was defective. (Paper No. 17.) The original appeal brief was not considered in deciding this appeal.

Here, claim 1 recites in pertinent part the following limitations: "a processor for controlling packet routing. . . ." Despite the appellants' argument, the claim does not require a router *per se*.<sup>4</sup> Giving the claim its broadest, reasonable construction, the limitations merely specify a processor for routing a packet.

## 2. Anticipation Determination

"Having construed the claim limitations at issue, we now compare the claims to the prior art to determine if the prior art anticipates those claims." *In re Cruciferous Sprout Litig.*, 301 F.3d 1343, 1349, 64 USPQ2d 1202, 1206 (Fed. Cir. 2002). "[A]nticipation is a question of fact." *Hyatt*, 211 F.3d at 1371, 54 USPQ2d at 1667 (citing *Bischoff v. Wethered*, 76 U.S. (9 Wall.) 812, 814-15 (1869); *In re Schreiber*, 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997)). "A claim is anticipated . . . if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (citing *Structural Rubber Prods. Co. v. Park Rubber Co.*, 749 F.2d 707, 715, 223 USPQ 1264, 1270

---

<sup>4</sup>Assuming *arguendo* that the claim did require a router *per se*, "[a]n anticipatory reference . . . need not duplicate word for word what is in the claims. Anticipation can occur when a claimed limitation is 'inherent' or otherwise implicit in the relevant reference." *Standard Havens Prods., Inc. v. Gencor Indus., Inc.*, 953 F.2d 1360, 1369, 21 USPQ2d 1321, 1328 (Fed. Cir. 1992) (citing *Tyler Refrigeration v. Kysor Indus. Corp.*, 777 F.2d 687, 689, 227 USPQ 845, 846-47 (Fed. Cir. 1985)). Here, the appellants admit that "[r]outers are . . . implicit in Aziz." (Supp. Appeal Br. at 8.)

(Fed. Cir. 1984); *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983); *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 771, 218 USPQ 781, 789 (Fed. Cir. 1983)).

Here, Aziz describes "communication between a node I coupled to private network 22, and a node J coupled to the private network 30, as shown in FIG. 2." Col. 6, ll. 59-61. The reference explains that nodes I and J can operate as "firewall machines coupled between their respective networks and the Internet 20." Col. 7, ll. 3-4. "For a description of . . . firewalls," *id.* at ll. 4-5, Aziz refers to and "incorporate[s] fully . . . by reference,"<sup>5</sup> col. 1, ll. 12-13, a patent application, which is now U.S. Patent No. 5,416,842 ("842 Patent"). Teaching that "firewalls (FWA) and (FWB) represent computers, such as the computer illustrated in FIG. 1," col. 5, ll. 34-37, the '842 Patent explains that each firewall "includes a central processing (CPU) 13. . . ." Col. 4, ll. 46-47.

"Coupl[ing] the computers of a private network to the Internet 20," '842 Patent, col. 4, l. 67 - col. 5, l. 1, each firewall "may thus act as a gatekeeper for messages and

---

<sup>5</sup>"[A]n application may . . . incorporate the content of another document or part thereof by reference to the document in the text of the specification. The information incorporated is as much a part of the application as filed as if the text was repeated in the application, and should be treated as part of the text of the application as filed." M.P.E.P. § 2163.07(b) (8th ed., rev. 1 Feb. 2003).

dam [sic] going to and from the Internet." *Id.* at col. 5, ll. 1-3. In acting as a gatekeeper, we find that each firewall's CPU routes packets between its respective private network and the Internet. For example, Aziz explains that node J's "[n]ormal packet processing may include the delivery to an appropriate local transport entity, or other outbound interface." Col. 11, ll. 11-13. Therefore, we affirm the rejection of claim 1.

Regarding claim 3, the appellants rely on their argument for claim 1. (Supp. Appeal Br. at 5.) Having found that argument unpersuasive, we affirm the rejection of claim 3.

#### B. CLAIMS 2, 11, 15, 25, 34, AND 35

Noting that "Aziz discloses that the public keys are included in the DH certificates which are issued by a multitier certificate structure which also tracks the ownership of IP addresses (col 16, line 60 - col 17, line 11)," (Supp. Examiner's Answer at 13), the examiner "infers that the certification authority of Aziz is also operating as a domain name server and binds public keys to IP addresses." (*Id.*) The appellants argue, "[i]n Aziz, a private key (group interchange key) is obtained from the group owner." (Supp. Appeal Br. at 6.) They further argue, "Aziz does not teach or suggest a domain name

server storing encryption keys," (*id.* at 7), and "Aziz does not teach or suggest a 'domain name server' with records that store a public key. . . ." (*id.* at 8.)

In addressing the point of contention, the Board conducts a two-step analysis. First, we construe the claims in question to determine their scope. Second, we determine whether the construed claims would have been obvious.

#### 1. Claim Construction

Claim 2 recites in pertinent part the following limitations: "said public key is obtained from a domain name server." Similarly, claim 11 recites in pertinent part the following limitations: "[a] domain name server comprising . . . a memory storing . . . a corresponding public key. . . ." Claim 15 recites in pertinent part limitations similar to those of claim 11. Giving claims 2, 11, and 15 their broadest, reasonable construction, the limitations require storing a **public** key on a domain name server and obtaining a **public** key therefrom.

Claim 25 recites in pertinent part the following limitations: "installing the public key for the multicast on a domain name sever [sic] or on a certification authority." Claim 34 recites similar limitations. Giving claims 25 and 34 their broadest, reasonable

construction, the limitations require storing a **public** key on a certification authority **or** on a domain name server.

## 2. Obviousness Determination

Having determined what subject matter is being claimed, the next inquiry is whether the subject matter would have been obvious. The question of obviousness is "based on underlying factual determinations including . . . what th[e] prior art teaches explicitly and inherently. . . ." *In re Zurko*, 258 F.3d 1379, 1386, 59 USPQ2d 1693, 1697(Fed. Cir. 2001) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966); *In re Dembiczak*, 175 F.3d 994, 998, 50 USPQ 1614, 1616 (Fed. Cir. 1999); *In re Napier*, 55 F.3d 610, 613, 34 USPQ2d 1782, 1784 (Fed. Cir. 1995)).

Here, Aziz "utilizes DH public-key certificates for key management, such that each IP source and destination is provided with a Diffie-Hellman public key. This DH public-key is distributed in the form of a certificate." Col. 8, ll. 12-15. Because these "certificates are issued by organizational [Certificate Authorities] CAs which have jurisdiction over the range of IP addresses that are being certified," col. 17, ll. 14-16, we find that public keys are stored therein and obtained therefrom. Because CAs have "the authority to bind a particular IP address to a DH public key," *id.* at ll. 6-7, moreover, we further find that these constitute domain name servers. Accordingly,

**public** keys are stored in and obtained from a domain name server, viz., a CA. The relevance of the appellants' argument whence "a **private** key . . . is obtained," (Supp. Appeal Br. at 6 (emphasis added)), escapes us. Therefore, we affirm the rejection of claims 2, 11, 15, 25, and 34.

Regarding claim 35, the appellants rely on their argument for claim 34. Having found the argument unpersuasive, we affirm the rejection of claim 35.

#### C. CLAIM 4

Observing that "Aziz discloses . . . transmitting and receiving multicasts . . . and further discloses that only group members would be authorized to send and receive multicasts (col 14, lines 11-17)," (Supp. Examiner's Answer at 6), the examiner "infers that messages to and from non-members (users which are not on the group membership list) would be blocked." (*Id.*) The appellants argue, "[i]n Aziz, no routing element is disclosed that does any decoding of a join request." (Supp. Appeal Br. at 6.)

Turning to Aziz, the reference discloses that "[w]hen secure multicasting to a multicast address M is required, a group membership creation primitive will establish the group key  $K_g$  and the membership list of addresses that are allowed to transmit and receive encrypted multicast datagrams to and from group address M." Col. 14, ll. 11-

17. Aziz explains that this "action will be taken by the group owner." *Id.* at ll. 17-18. Accordingly, "[n]odes wishing to transmit/receive encrypted datagrams to multicast address M," *id.* at ll. 23-24, must "send[] an encrypted/authenticated request-to-join primitive to the group owner." *Id.* at ll. 25-26. We find that the group owner decrypts, i.e., decodes, the encrypted request-to-join primitive to determine "[i]f the requesting node's address is part of the group's authorized membership list. . . ." *Id.* at ll. 26-28. If the address is part of the list, the group owner routes "the GIK  $K_g$ , algorithm identifier, associated lifetime information and key-change policy in an encrypted packet. . . ." *Id.* at ll. 28-32. Therefore, we affirm the rejection of claim 4.

#### D. CLAIM 5

The examiner finds, "Aziz discusses establishing and joining closed (private) multicast groups (subspaces)." (Supp. Examiner's Answer at 7.) The appellants argue, "[i]n the claim, there are separate address spaces for private and public multicasts, Aziz does not teach a separate address space for private multicasts." (Supp. Appeal Br. at 7.)

#### 1. Claim Construction

"[L]imitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184, 26 USPQ2d 1057, 1059 (Fed. Cir. 1993) (citing *In re*

*Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989)). Here, claim 5 recites in pertinent part the following limitations: "a private multicast address space." Contrary to the appellants' argument, the claim does not require "separate address spaces for private and public multicasts. . . ." (Supp. Appeal Br. at 7.) Giving the claim its broadest, reasonable construction, the limitations merely specify an address space for a private multicast.

## 2. Anticipation Determination

We find that Aziz discloses an address space for a private multicast. As aforementioned, "[w]hen secure multicasting to a multicast address M is required, a group membership creation primitive will establish . . . the membership list of addresses that are allowed to transmit and receive encrypted multicast datagrams to and from group address M." Col. 14, ll. 11-17. The membership list of addresses constitutes an address space for participating in a private multicast by transmitting and receiving encrypted multicast datagrams to and from group address M. Therefore, we affirm the rejection of claim 5.

## E. CLAIMS 6, 21, 30, AND 31

Admitting that "Aziz . . . does not explicitly disclose using a bit-mask to indicate groups of senders permitted to communicate with or not communicate with the

communications port," (Supp. Examiner's Answer at 11), the examiner asserts, "*Henrion* uses bit masks to identify one or more routing groups so as to allow or block senders from communicating with the communicate port (col 16, lines 57-60 and col 17, line 63 - col 18, line 8)." (*Id.* at 23.) The appellants argue, "[i]n *Henrion et al.*, the bit masks are used to identify groups of output ports of a switch that are involved in a multicast tree." (Supp. Appeal Br. at 10-11.)

#### 1. Claim Construction

Claim 6 recites in pertinent part the following limitations: "the processor is configured to block multicast packets received from senders blocked from sending to a receiver as indicated by a bit-mask received with a multicast join request." Similarly, claim 21 recites in pertinent part the following limitations: "sending a list of bit-masks specifying at least one of a group of senders permitted to send to said user and a group of senders prohibited from sending to said user." Also similarly, claim 30 recites in pertinent part the following limitations: "sending a group specific multicast join request including a bit-mask specifying at least one of a group of senders permitted to send to said user and a group of senders prohibited from sending to said user." Giving claims 6, 21, and 30, their broadest, reasonable construction, the limitations require a bit-mask specifying at least one of a group of senders prohibited from sending to a receiver.

## 2. Obviousness Determination

"In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)). "a *prima facie* case of obviousness is established when the teachings from the prior art itself would . . . have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell*, 991 F.2d 781, 783, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)).

Here, although the passage of Henrion cited by the examiner discloses "an 8-bit mask word MSK," col. 17, ll. 66-67, we are unpersuaded that the mask word specifies, or would have suggested specifying, at least one of a group of senders prohibited from sending to a receiver. To the contrary, the MSK "identif[ies] the different routing groups to which a copy [of a cell] is to be sent. . . ." Col. 16, ll. 59-60. Therefore, we reverse the rejection of claim 6; of claim 21; of claim 30; and of claim 31, which depends from the latter.

F. CLAIMS 7-10, 19, 20, 28, and 29

The examiner asserts, "Aziz discloses . . . [a] processor which sends a private multicast join request (col 14, lines 25-26) comprising a first information and an encrypted first information (col 14, lines 50-55)." (Supp. Examiner's Answer at 6.) The appellants argue, "[a]s set forth in column 14, lines 50-55, the actual IP multicast address for which a join request is submitted is sent. It is either sent in the clear or encrypted, but not both." (Supp. Appeal Br. at 8.)

1. Claim Construction

Claim 7 recites in pertinent part the following limitations: "said processor configured to send a private multicast join request comprising first information and encrypted first information." Claims 19 and 28 recite similar limitations. Giving claims 7, 19, and 28 their broadest, reasonable construction, the limitations require that a private multicast join request include a datum in both unencrypted form and encrypted form.

2. Anticipation and Obviousness Determinations

"[A]bsence from the reference of any claimed element negates anticipation." *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1571, 230 USPQ 81, 84 (Fed. Cir. 1986). Here, the passages of Aziz cited by the examiner describe "[t]he packet

formats for the GIK request/response. . . ." Col. 14, ll. 34-35. Therein, "[t]he first field specifies the version of this protocol, which is 1. Following this field is the actual IP multicast address for which the GIK is being requested." *Id.* at ll. 49-51. Although "[t]he request packet . . . may optionally be encrypted," *id.* at l. 53, we are unpersuaded that the request packet may include a datum in both unencrypted form and encrypted form. To the contrary, we agree with the appellants that the packet "is either sent in the clear or encrypted, but not both." (Supp. Appeal Br. at 8.) Therefore, we reverse the rejection of claim 7; of claim 8, which depends therefrom; of claim 19; and of claim 28.

Furthermore, the examiner does not allege, let alone show, that the addition of Herz or Henrion cures the aforementioned deficiency of Aziz. Therefore, we reverse the rejections of claims 9 and 10, which depend from claim 7; of claim 20, which depends from claim 19; and of claim 29, which depends from claim 28.

#### G. CLAIM 12

Observing that "Aziz further discloses sending and receiving information from a (multicast) group owner (col 14, lines 4-17)," (Supp. Examiner's Answer at 8), the examiner "infers that the group owner's address and the multicast address (col 14, line 12) has been previously stored in the memory." (*Id.*) The appellants argue, "Aziz

has no teaching or suggestion of a domain name server that has 'records [that] include an indication of an owner of a multicast'. . . ." (Supp. Appeal Br. at 7.)

### 1. Claim Construction

Claim 12 recites in pertinent part the following limitations: "records include an indication of an owner of a multicast." Giving the claim its broadest, reasonable construction, the limitations require storing an indication of an owner of a multicast and storing an indication distinguishing whether a multicast is public or private.

### 2. Obviousness Determination

As mentioned regarding claim 4, Aziz discloses that "[w]hen secure multicasting to a multicast address M is required, a group membership creation primitive will establish the group key  $K_g$  and the membership list of addresses that are allowed to transmit and receive encrypted multicast datagrams to and from group address M." Col. 14, ll. 11-17. This "action will be taken by the group owner." *Id.* at ll. 17-18. Once the group key and membership list are established, "[n]odes wishing to transmit/receive encrypted datagrams to multicast address M," *id.* at ll. 23-24, "send[] an encrypted/authenticated request-to-join primitive to the group owner." *Id.* at ll. 25-26. Because storing an indication of the respective owners of multicasts would have enabled a node wishing to participate in a specific multicast to identify which owner to whom to send a

request-to-join, we are persuaded that teachings from the prior art would have suggested storing an indication of an owner of a multicast. Therefore, we affirm the rejection of claim 12.

#### H. CLAIM 13

Recognizing Aziz "does not explicitly disclose that an indication of whether the multicast is public or private is included in the records," (Supp. Examiner's Answer at 8), the examiner takes official notice that "[i]t is old and well known within the computer arts to store such information in distributed databases using standard crosslinking methods to identify linked files." (*Id.*) He asserts, "it would have been obvious to one having ordinary skill in the art at the time of the invention to store the records in a distributed database and to include an indication in each record denoting the multicast group(s) that the record was a part of [sic]." (*Id.*) The examiner explains, "[o]ne would have been motivated to include such an indication in order to provide more efficient use of the memory storage space by precluding the need to have duplicate copies of the record in every public and/or private multicast group to which it belongs." (*Id.* at 8-9.) The appellants argue, "Aziz has no teaching or suggestion . . . of 'records that include an indication distinguishing whether a multicast is public or private'. . . ." (Supp. Appeal Br. at 7.)

### 1. Claim Construction

Claim 13 recites in pertinent part the following limitations: "said records include an indication distinguishing whether a multicast is public or private." Giving the claim its broadest, reasonable construction, the limitations require storing an indication to distinguish whether a multicast is public or private.

### 2. Obviousness Determination

As mentioned regarding claim 4, Aziz discloses that "[w]hen secure multicasting to a multicast address M is required, a group membership creation primitive will establish the group key  $K_g$  and the membership list of addresses that are allowed to transmit and receive encrypted multicast datagrams to and from group address M." Col. 14, ll. 11-17. This "action will be taken by the group owner." *Id.* at ll. 17-18. Because permission must be obtained to join the secure multicast, we find that the multicast is "private." Conversely, we find that a multicast that requires no such permission to join is public.

Once established, the group key must be stored for reference. We find that storing the key for private multicasts distinguishes such multicasts from those public multicasts for which no key is needed. Therefore, we affirm the rejection of claim 13.

I. CLAIMS 14, 17, 22, 32, AND 33

"[T]o assure separate review by the Board of individual claims within each group of claims subject to a common ground of rejection, an appellant's brief to the Board must contain a clear statement for each rejection: (a) asserting that the patentability of claims within the group of claims subject to this rejection do not stand or fall together, and (b) identifying which individual claim or claims within the group are separately patentable and the reasons why the examiner's rejection should not be sustained." *In re McDaniel*, 293 F.3d 1379, 1383, 63 USPQ2d 1462, 1465 (Fed. Cir. 2002) (citing 37 C.F.R. §1.192(c)(7) (2001)). "If the brief fails to meet either requirement, the Board is free to select a single claim from each group of claims subject to a common ground of rejection as representative of all claims in that group and to decide the appeal of that rejection based solely on the selected representative claim." *Id.*, 63 USPQ2d at 1465.

Here, the appellants stipulate that claims 14 and 17 stand or fall together. (Supp. Appeal Br. at 5.) We select claim 14 as representative thereof. With this representation in mind, we address the point of contention.

The examiner reasons, "*Aziz* discusses establishing and joining closed (private) multicast groups . . . (col 14, lines 4-17), thus inferring [sic] that entities outside of the closed groups would be considered public groups. . . ." (Supp. Examiner's Answer

at 18.) He adds, "[s]ince some multicast groups are private (closed) and some are public (open) in *Aziz*, once the identity of the multicast group was determined, it follows that the type of group would also be known." (*Id.* at 17.) The appellants argue, "[a]ny routers implicit in *Aziz* do not distinguish between public and private multicasts. . . ." (Supp. Appeal Br. at 7.)

### 1. Claim Construction

Claim 14 recites in pertinent part the following limitations: "at least one routing element, connecting at least two sub-networks, configured to distinguish between public and private multicasts." Giving the representative claim its broadest, reasonable construction, the limitations require that at least one routing element distinguish between public and private multicasts.

Claim 22 recites in pertinent part the following limitations: "determining whether the request relates to a public or private multicast." Claim 32 recites similar limitations. Giving claims 22 and 32 their broadest, reasonable construction, the limitations require determining whether a join request relates to a public or private multicast.

## 2. Anticipation Determination

As mentioned regarding claim 4, Aziz discloses that "[w]hen secure multicasting to a multicast address M is required, a group membership creation primitive will establish the group key  $K_g$  and the membership list of addresses that are allowed to transmit and receive encrypted multicast datagrams to and from group address M." Col. 14, ll. 11-17. "Nodes wishing to transmit/receive encrypted datagrams to multicast address M," *id.* at ll. 23-24, must "send[] an encrypted/authenticated request-to-join primitive to the group owner." *id.* at ll. 25-26. Because the group owner exercises discretion to authorize or deny a request to join his secure multicast, we find that the multicast is "private." Conversely, we find that a multicast that is open for anyone to join is public. Accordingly, the reference must determine whether a join request relates to a public or a private multicast. Therefore, we affirm the rejection of claims 22 and 32.

Regarding claim 33, the appellants rely on their argument for claim 32. Having found the argument unpersuasive, we affirm the rejection of claim 33.

Returning to Aziz, encrypted multicast packets used in the private multicasts include a "destination IP address . . . used by the receiver to determine whether to use unicast or multicast key-processing procedures on a received IP packet. In case [sic]

the destination address is an IP multicast address, it will use the group IK [sic]  $K_g$  to decrypt the packet encryption key  $K_p$ ." Col. 15, ll. 55-59.

As mentioned regarding claim 1 and 3, nodes operating as firewalls route packets. The appellants admit, moreover, that "[r]outers are . . . implicit in Aziz." (Supp. Appeal Br. at 8.) Accordingly, we find that the firewalls or the implicit routers use the aforementioned destination IP address to distinguish between public and private multicasts. Therefore, we affirm the rejection of claim 14 and of claim 17, which falls therewith.

#### J. CLAIM 16

Noting that "Aziz discloses that the public keys are included in the DH certificates which are issued by a multi-tier certificate structure which also tracks the ownership of IP addresses (col 16, line 60 - col 17, line 11)," (Supp. Examiner's Answer at 18), the examiner "infers that the certification authority of Aziz . . . binds public keys to IP addresses." (*Id.*) The appellants argue, "Aziz does not teach or suggest . . . a 'certification authority' storing 'records relating to a network address or alias with a public key'. . . ." (Supp. Appeal Br. at 8.)

### 1. Claim Construction

Claim 16 recites in pertinent part the following limitations: "a certification authority, connected to a sub-network, storing records relating a network address or alias with a public key of a public/private key encryption pair." Giving the claim its broadest, reasonable construction, the limitations require that a certification authority store records relating a network address or alias with a public key.

### 2. Obviousness Determination

As mentioned regarding claims 2, 11, 15, 25, 34, and 35; we found that Aziz's Certificate Authorities (CAs), "hav[ing] jurisdiction over the range of IP addresses that are being certified," col. 17, ll. 14-16, store public keys. As also aforementioned, CAs have "the authority to bind a particular IP address to a DH public key." *Id.* at ll. 6-7. Because storing a record of the binding of a particular IP address to a DH public key would have memorialized the binding, we are persuaded that teachings from the prior art would have suggested that a CA store records relating a network address or alias with a public key. Therefore, we affirm the rejection of claim 16.

### K. CLAIMS 18, 26, AND 27

The examiner asserts, "[b]y creating one or more closed multicast groups, Aziz is partitioning the total multicast address space into subspaces." (Supp. Examiner's

Answer at 18.) The appellants argue, "Aziz does not partition a multicast address space at all." (Supp. Appeal Br. at 8.)

### 1. Claim Construction

Claim 18 recites in pertinent part the following limitations: "providing a multicast address space having a subspace for public multicasts and a subspace for private multicasts." Claim 26 recites similar limitations. Giving claims 18 and 26 their broadest, reasonable construction, the limitations require partitioning a multicast address space into a subspace for public multicasts and a subspace for private multicasts.

### 2. Anticipation and Obviousness Determinations

"To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (quoting *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749 (Fed. Cir. 1991))

"Inherency . . . may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *In re Oelrich*, 666 F.2d 578, 581, 212 USPQ 323, 326 (CCPA 1981) (citing *Hansgirk v. Kemmer*, 102 F.2d 212, 214, 40 USPQ 665, 667 (1939)).

Here, although Aziz creates a closed multicast group "[w]hen secure multicasting to a multicast address M is required," col. 14, ll. 11-12, we are unpersuaded that such creation necessitates or would have suggested partitioning a multicast address space into a subspace for public multicasts and a subspace for private multicasts. Therefore, we reverse the rejections of claim 18, of claim 26, and of claim 27, which depends from the latter.

#### L. CLAIMS 23 AND 24

The examiner makes the following findings.

*Aziz* discloses a method and apparatus for transmitting and receiving multicasts, comprising a router (node) with: a.[i]Input and output ports (col 6, lines 28-34); and b. [a] processor for controlling the routing by: (1) obtaining a public key (col 11, lines 1-5); (2) decoding an encrypted portion of the multicast join request received from a user (col 11, lines 7-9); and (3) verifying that the user is authorized to join the multicast (col 14, lines 19-32).

(Supp. Examiner's Answer at 5.) The appellants argue, "Aziz does not teach or suggest using a public key or decryption at a router as required by claims 23 and 24." (Supp. Appeal Br. at 8.)

#### 1. Claim Construction

"Generally, . . . the preamble does not limit the claims." *DeGeorge v. Bernier*, 768 F.2d 1318, 1322 n.3, 226 USPQ 758, 761 n.3 (Fed. Cir. 1985). In particular,

"[t]he preamble of a claim does not limit the scope of the claim when it merely states a purpose or intended use of the invention." *In re Paulsen*, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994) (citing *DeGeorge*, 768 F.2d at 1322 n.3, 226 USPQ at 761 n.3). "Where . . . the effect of the words [in the preamble] is at best ambiguous . . . a compelling reason must exist before the language can be given weight." *Arshal v. United States*, 621 F.2d 421, 430-31, 208 USPQ 397, 406-07 (Ct. Cl. 1980) (citing *In re de Castelet*, 562 F.2d 1236, 1244 n.6, 195 USPQ 439, 447 n.6 (CCPA 1977)).

Here, the word "router" appears only in the preamble of claim 22, from which claim 23 depends. The word merely states a purpose or intended use of the claimed "method of processing." The bodies of claims 22-24 neither repeat nor reference the word; instead, the bodies specify steps of the method. Because the language in the bodies of the claims standing alone is clear and unambiguous, we find no compelling reason to give the word weight. Therefore, the part of appellants' argument that relies on the word not persuasive. The remaining, material part of the argument is that "Aziz does not teach or suggest using a public key or decryption. . . ." (Supp. Appeal Br. at 8.)

## 2. Anticipation Determination

Because "the firewall servers are Internet protocol (IP) server computers which . . . encrypt and **decrypt** datagram traffic sent and received to nodes on the private networks over the Internet 20," '842 Patent, col. 5, ll. 7-11 (emphasis added), we find that the firewalls of Aziz perform decryption. We also find that the firewalls use public keys. Specifically, "the use of Diffie-Hellman (DH) **public-key** certificates can avoid the pseudo session state establishment. . . ." '842 Patent, col. 6, ll. 17-19. Therefore, we affirm the rejection of claims 23 and 24.

## CONCLUSION

In summary, the rejection of claims 1, 4, 5, 14, 17, 19, 22-24, and 32 under § 102(e) is affirmed. In contrast, the rejection of claims 7, 8, 18, 26, 28 under § 102(e) is reversed. The rejections of claims 2, 3, 11-13, 15, 16, 25, and 33-35 under § 103(a) as obvious are affirmed. In contrast, the rejections of claims 6, 9, 10, 20, 21, 27, 29, 30, and 31 under § 103(a) are reversed.

"Any arguments or authorities not included in the brief will be refused consideration by the Board of Patent Appeals and Interferences. . . ." 37 C.F.R. § 1.192(a). Accordingly, our affirmance is based only on the arguments made in the brief(s). Any arguments or authorities not included therein are neither before us nor at issue but are considered waived.

No time for taking any action connected with this appeal may be extended under  
37 C.F.R. § 1.136(a).

AFFIRMED-IN-PART

MICHAEL R. FLEMING  
Administrative Patent Judge

JOSEPH L. DIXON  
Administrative Patent Judge

LANCE LEONARD BARRY  
Administrative Patent Judge

)  
)  
)  
)  
)  
) BOARD OF PATENT  
) APPEALS  
) AND  
) INTERFERENCES  
)  
)  
)  
)

Appeal No. 2002-1527  
Application No. 08/885,817

Page 31

ROSENTHAL & OSHA L.L.P. / SUN  
1221 MCKINNEY, SUITE 2800  
HOUSTON, TX 77010