

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EMC CORPORATION, EMC INTERNATIONAL U.S. HOLDINGS, INC.,
and VMWARE, INC.,
Petitioner,

v.

CLOUDING CORP.,
Patent Owner.

Case IPR2014-01216
Patent 5,825,891

Before JAMESON LEE, JUSTIN BUSCH, and KRISTINA M. KALAN,
Administrative Patent Judges.

KALAN, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

A. *Background*

EMC Corporation, EMC International U.S. Holdings, Inc., and VMware, Inc., (collectively, “Petitioner”) filed a Petition requesting *inter partes* review of claims 1–8 of U.S. Patent 5,825,891 (Ex. 1001, “the ’891 patent”) pursuant to 35 U.S.C. §§ 311–319. Paper 1 (“Pet.”). Clouding Corp. (“Patent Owner”) filed a Preliminary Response. Paper 11. On January 26, 2015, we instituted an *inter partes* review of claims 1–8 on certain grounds of unpatentability alleged in the Petition. Paper 12 (“Dec.”). After institution of trial, Patent Owner filed a Patent Owner Response (Paper 25; “PO Resp.”) and Petitioner filed a Reply (Paper 29; “Reply”). An oral hearing was held on August 17, 2015. A transcript of the hearing has been entered into the record. Paper 39 (“Tr.”).

The Board has jurisdiction under 35 U.S.C. § 6(c). In this Final Written Decision, issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73, we determine that Petitioner has shown by a preponderance of the evidence that all claims for which trial is instituted, namely, claims 1–8, are unpatentable.

B. *The ’891 Patent*

The ’891 patent is related to a method for enabling computers to communicate using encrypted network packets. Ex. 1001, Abs. In particular, the ’891 patent discloses a method for generating tunnel records and a method for updating tunnel records. Ex. 1001, 6:5–52.

C. *Related Matters*

Patent Owner identifies the following related district court proceeding between Petitioner and Patent Owner that involves the ’891 patent:

Clouding Corp. v. EMC Corp., Case No. 1:14-cv-01178 (D. Del.). Paper 9, 2; Paper 10, 2. Petitioner and Patent Owner identify also the following *inter partes* reviews, involving different petitioners than the present Petition, that were before the Board involving the '891 patent, but are now terminated: IPR2013-00100, IPR2013-00260, and IPR2014-00308. Pet. 4; Paper 9, 2.

D. Illustrative Claims

Independent claims 1 and 6 are reproduced below:

1. A method for enabling computers to communicate using encrypted network packets, comprising:
 - sending a configuration request over a network from a first computer to a second computer;
 - providing a temporary configuration password to the first computer;
 - encrypting, in accordance with the temporary configuration password, tunnel record information that includes a secret tunnel encryption key assigned to a tunnel between the first computer and the second computer; and
 - sending the tunnel record information over the network from the second computer to the first computer.

Ex. 1001, 7:2–15;

6. A method for updating a tunnel record, comprising:
 - sending a connection request from a first computer to a second computer;
 - authenticating the first computer; and
 - updating a tunnel record corresponding to the connection request with the first computer's network address.

Id. at 8:1–7.

E. Prior Art References Applied by Petitioner

Petitioner challenges the patentability of claims 1–8 based on obviousness in view of the following references:

Aziz	US 5,416,842	May 16, 1995	(Ex. 1005)
Rodwin	US 5,812,819	Sept. 22, 1998	(Ex. 1008)
Weiss	WO 87/05175	Aug. 27, 1987	(Ex. 1009)

Charlie Kaufman *et al.*, *Network Security: Private Communication in a Public World* (1995) (Ex. 1007) (“Kaufman”).

F. Instituted Grounds of Unpatentability

1. Claims 1–5 as unpatentable under 35 U.S.C. § 103(a) over Aziz and Kaufman;
2. Claims 1–5 as unpatentable under 35 U.S.C. § 103(a) over Aziz and Weiss;
3. Claims 6–8 as unpatentable under 35 U.S.C. § 103(a) over Aziz and Rodwin.

II. ANALYSIS

A. Claim Construction

The Board interprets claims in an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1277–79 (Fed. Cir. 2015), *reh’g en banc denied*, 2015 WL 4100060 (Fed. Cir. July 8, 2015) (“We conclude that Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA.”). Under that construction, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire patent disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Claim terms generally are given their ordinary and customary meaning, unless it appears from the specification or

the file history that they were used differently by the inventor, in a clear, deliberate, and precise manner. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

In the Decision to Institute, we construed the terms “temporary configuration password,” “authenticating,” “tunnel record,” and “tunnel record information.” Dec. 6–12. As is pertinent to our discussion below, we construed “authenticating” as “a process which validates a computer or user.” *Id.* at 11.

Patent Owner does not dispute the Board’s claim construction nor advance an alternative construction. Petitioner argues that Patent Owner’s expert recites the Board’s constructions and affirms that he is applying them. Reply 3–4. Accordingly, Petitioner urges, the Board should adopt its earlier constructions in its final determination. *Id.* at 4. Based on considering anew the complete record now before us, we see no reason to alter our earlier constructions, and maintain the constructions for this Final Written Decision. We see no need to construe expressly any other claim limitations.

B. Claims 1–5 as Obvious over Aziz and Kaufman and Aziz and Weiss

Petitioner contends that claims 1–5 would have been obvious over Aziz and Kaufman and over Aziz and Weiss. Pet. 46–54. Patent Owner disagrees. PO Resp. 7–20.

1. Aziz (Ex. 1005)

Aziz describes a method to perform secure *tunneling* for encrypting data packets between computers. Ex. 1005, 1:5–11, 6:3–15. According to Aziz, there are several security advantages to tunneling—a technique that encrypts the entire original Internet Protocol (IP) packet, rather than only the

data portion of the IP packet. *Id.* Notably, Aziz explains that tunneling prevents the topology and the number of nodes in the private network from being discovered by a hacker. *Id.* When transmitting an IP packet using tunneling, all an unintended observer can determine is that there are a certain number of firewalls that communicate with each other, and no information, either as to which nodes in the private network are communicating on an end-to-end basis or as to the number of nodes that exist in the private network, is revealed to unintended observers. *Id.*

Aziz further describes several network schemes that utilize its invention. For instance, Figure 2 of Aziz, reproduced below, illustrates Internet 20 coupled to private network 22 through a firewall server FWA:

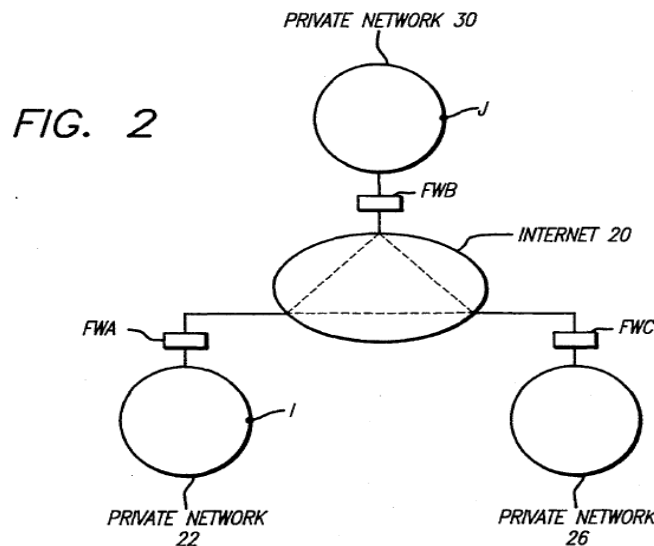


Figure 2 of Aziz diagrammatically illustrates one possible network scheme using the teachings of the invention in an Internet environment. Ex. 1005, 2:54–56. As shown in Figure 2 of Aziz, each private network (22, 26, and 30) is coupled to Internet 20 through a firewall server (FWA, FWC, and FWB, respectively). *Id.* at 4:65–5:16. The firewall servers are IP server computers, which encrypt and decrypt data packets or datagrams sent and

received to nodes on the private networks over Internet 20. For example, when node I on private network 22 sends a packet to node J on private network 30, firewall server FWA first determines that node J is coupled to network 30, and that firewall server FWB serves network 30. *Id.* at 5:54–6:2. Then, firewall server FWA encapsulates the original IP data packet (header and data) and transmits the data packet in an encrypted IP packet intended for remote firewall FWB. *Id.*

In another embodiment, Aziz describes a portable computer that connects to a public network where the computer is assigned an IP address dynamically. Ex. 1005, 10:37–11:53, Fig. 8. In that situation, Aziz utilizes a tunneling scheme in which the cryptographic credentials are associated with the inner IP address. *Id.*

2. Kaufman (Ex. 1007)

Kaufman describes a network authentication scheme, specifically a technique for distributing keys in a secure manner. Ex. 1007, 266–269.¹ Figure 10-1 of Kaufman, reproduced below, illustrates Kaufman’s key distribution technique (Ex. 1007, 269):

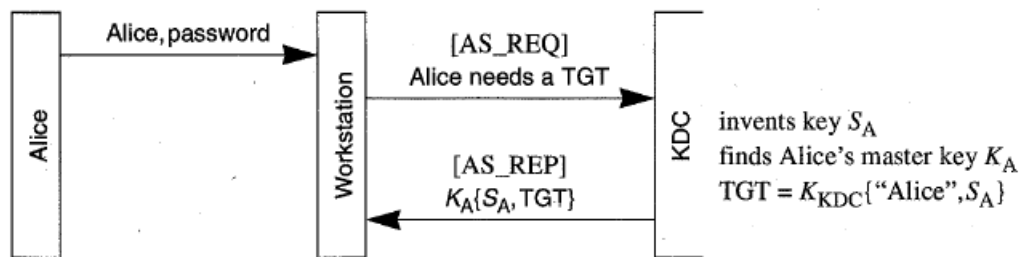


Figure 10-1. Obtaining a TGT

¹ The page numbers in our citation to Kaufman are the original page numbers in the textbook, on the top right and left corners of each page.

Figure 10-1 illustrates Kaufman's described process of "Obtaining a TGT." *Id.* at 269. As shown in Figure 10-1 of Kaufman, Alice (a user) logs into the workstation by entering *her name and password*. *Id.* at 266. To minimize security risk, the workstation asks the server (Key Distribution Center (KDC)) for a *session key S_A* for Alice to use for just this one session. *Id.* Kaufman's system derives Alice's *master key* from her password. *Id.* The KDC generates a session key S_A and transmits S_A (encrypted with Alice's master key) to the workstation. *Id.* The KDC also sends a ticket-granting ticket (TGT), which is S_A (and other information, such as Alice's name and the TGT's expiration time) encrypted with the KDC's master key. *Id.* The workstation uses Alice's master key (derived from her password) to decrypt the encrypted S_A . *Id.* at 267. After that, the workstation forgets Alice's password and only remembers S_A and the TGT. *Id.* When Alice later needs to access a remote resource, *her workstation transmits the TGT, which includes S_A , to KDC*, along with the name of the resource to which Alice needs a ticket. *Id.*

3. Weiss (Ex. 1009)

Weiss describes a method for distributing encryption key codes from a central data site to remote access units. Ex. 1009, 1:1–5. Weiss describes a randomly generated source number that is used to generate a master key digital code number. *Id.* at 17:13–15. The master key code may be used to transfer additional keys securely over an insecure channel connecting the computers. *Id.* at 39:27–40:7. The random source numbers are destroyed to prevent discovery through re-computation of the master key codes. *Id.* at 20:3–9, 23:2–9.

4. *Analysis*

After considering the Petition, Patent Owner Response, Reply, and all evidence relied on by Petitioner and Patent Owner, we are persuaded that Petitioner has shown, by a preponderance of the evidence, that claims 1–5 would have been obvious over Aziz and Kaufman and over Aziz and Weiss. The Petition sufficiently accounts for each of the elements in these claims and provides well-supported reasons to combine the prior art teachings to satisfy the claim elements.

Patent Owner challenges Petitioner’s contention that Aziz’s “firewall-to-firewall” communication scheme can be modified using the Kerberos key exchange technique described by Kaufman. PO Resp. 9–10. Specifically, Patent Owner argues Aziz seeks to avoid, and counsels readers against, the type of key exchange taught by Kaufman. *Id.* at 11. Patent Owner also challenges Dr. Reynolds’s statement that one of ordinary skill in the art would have recognized the advantages of using a private key to encrypt communications as described by Kaufman in place of the public key encryption described in Aziz because it involves a key that is smaller in size, a key that takes less computational effort in the encryption/decryption process, and a key that eliminates the need for public maintenance. *Id.* Patent Owner maintains that Dr. Reynolds “fails to convincingly explain *why* any person of ordinary skill in the art would employ such keys in a system as taught by Aziz.” *Id.* at 12. Patent Owner summarizes that “[o]ur argument is that the combination that the Petitioners have proposed is not a combination that would be made and, therefore, the obviousness argument is not a legally sound argument.” Tr. 61:17–20.

Petitioner argues, first, that Patent Owner does not dispute that the prior art teaches all the elements of claims 1–5. Reply 4–5; Tr. 10:17–19. Petitioner argues, next, that a person of ordinary skill in the art would have combined the teachings of Aziz and Kaufman, or Aziz and Weiss, because they all relate to techniques for secure computer communications, and teach key distribution techniques. Reply 6 (citing Ex. 1028 ¶¶ 9–18). Petitioner relies on the testimony of Dr. Reynolds, who opines that there are numerous advantages to be had by using a private key, as in Kaufman and Weiss, in place of the public key encryption described in Aziz:

[S]ome advantages of using a private key over a public key include a key that is smaller in size, a key that takes less computational effort to encrypt, and a key that eliminates the need for public maintenance.

Ex. 1020 ¶¶ 54, 68; Ex. 1028 ¶¶ 12–14. Dr. Reynolds further explains that making such combinations would not have been beyond the skill level of one of ordinary skill in the art, and would not yield more than predictable results. Ex. 1028 ¶ 10. Petitioner argues that even Patent Owner’s expert confirmed that one of ordinary skill in the art would have been familiar with private key schemes, public key schemes, and their relative advantages. Reply 9–10. In sum, Petitioner argues that “one of ordinary skill in the art would have been motivated to replace the public key encryption described in Aziz with the private key technique described in Kaufman and Weiss, especially if, in a particular network, the need for encryption/decryption performance outweighed the advantage of public keys.” *Id.* at 11.

As noted by Petitioner, there is no dispute on the claim construction, and there is no dispute that the combination of Aziz and Kaufman or Aziz and Weiss meets every element of claims 1 through 5. Reply 1; Tr. 10:15–

19. Thus, the dispute regarding claims 1–5 reduces to whether one of ordinary skill in the art would have combined the necessary elements of Aziz with Kaufman or Weiss to yield the claimed subject matter. In this regard, we are persuaded by Petitioner’s arguments that one of ordinary skill in the art would have combined Aziz with Kaufman or Weiss to arrive at the claimed invention.

Preliminarily, Petitioner argues that the claims themselves “don’t require either public or private key approaches. They are agnostic on that.” Tr. 13:10–11. We agree with Petitioner that the claims do not require or prohibit use of one or the other of a private key or a public key approach. Aziz, in its teaching of a method to perform secure tunneling for encrypting data packets between computers, discusses use of a key management scheme to encrypt those data packets, i.e., the “public key” technique referred to by Petitioner. Ex. 1005, 1:5–11; 6:16–40; Ex. 1020 ¶ 49.

Regarding the combination of Aziz’s methods with the “private key” technique of Kaufman and Weiss, we credit the testimony of Petitioner’s expert, Dr. Reynolds, that using a private key technique, as in Kaufman and Weiss, in place of a public key technique would have had advantages known to those of ordinary skill in the art. Ex. 1020, ¶¶ 54, 68; Ex. 1028 ¶¶ 12–14. Patent Owner’s expert, Dr. Nettles, agreed that “there are advantages and disadvantages to public- and secret-key encryption schemes” and that they would have been understood by a person of ordinary skill in the art at the time of the ’891 patent. Ex. 1027, 34:5–15, 42:11–16; Tr. 19:1–9, 21:18–24. Patent Owner’s expert also agreed that, in general, at the time of the ’891 patent, “a person of ordinary skill in the art could have implemented a system using either public-key or private-key techniques.” *Id.* at 41:15–20.

Accepting that one of ordinary skill in the art would have known of the relative advantages of the public-key and private-key techniques, and how to implement a system using either technique, it follows that one of ordinary skill in the art would have known to use in the system of Aziz the private-key technique of Kaufman and/or Weiss to obtain the benefits of using a private-key technique.

We also agree with Petitioner's argument that replacing a public key with a private key would have been an alternative technique known to one of ordinary skill in the art. Reply 11; Ex. 1028 ¶ 14; Tr. *passim*. Petitioner's expert opined that, depending on the relative needs of the particular network — either security and efficiency, or allowing encrypted communication between parties that do not already share a secret — a person of ordinary skill in the art would have been motivated to choose either a public key or a private key system design. Ex. 1028 ¶ 14; Tr. 72:17–73:2. Patent Owner's expert did not counter that the combination of Aziz and Kaufman would yield unpredictable results. Ex. 1027, 63:2–18. Aziz does not, based on the information before us, prohibit a design that includes a private key arrangement. We note that Aziz itself teaches that its system could be used in other network arrangements. Ex. 1005, 5:11–16; 10:37–11:53; 11:55–12:11. Petitioner's expert opines that this teaching in Aziz would have motivated a person of ordinary skill in the art to combine the teachings of Aziz with either Kaufman or Weiss. Ex. 1028 ¶ 15. Given that one of ordinary skill in the art would have known about the relative advantages of the public-key and private-key techniques, and also of situations in which one might be preferred over the other, we agree with Petitioner that one of

ordinary skill in the art would have been motivated to combine Aziz with Kaufman and/or Weiss.

Patent Owner does not argue persuasively to the contrary. Although Patent Owner argues that Aziz seeks to avoid, and counsels readers against, the type of key exchange taught by Kaufman, Patent Owner does not reconcile this with Aziz's statement that Aziz's system could be used in other network arrangements. Nor does Patent Owner's expert provide adequate reasoning to counter Petitioner's assertion that one of ordinary skill in the art would have used a private key exchange in the system of Aziz.

Patent Owner relies on assertions made by its expert that, in Kaufman and Weiss, both computers would need to be operational to exchange private key information successfully. PO Resp. 10; Ex. 2002 ¶¶ 18, 24. Petitioner explains, persuasively, how neither Kaufman nor Weiss actually requires that both computers would need to be operational in order to exchange private key information successfully. Tr. 15:21–16:18; 16:24–17:11; Ex. 1028 ¶ 16. Patent Owner also argues that Aziz prefers use of DH public key certificates over other methods. PO Resp. 8. This section of Aziz expresses a preferred embodiment and does not preclude or advocate affirmatively against using other methods. Additionally, as explained by Petitioner's expert, this section contrasts DH public key certificate methods with other public key certificate methods such as RSA; it does not contrast DH public key certificate methods with private key methods. Ex. 1028 ¶ 17.

Given the totality of the arguments, one of ordinary skill in the art would have known that the design of the Aziz system could have been modified to include a private key system to encrypt communications, and would have been motivated to do so to capitalize upon the advantages of the

private key system. Upon review of the complete record, we find that Petitioner has established, by a preponderance of the evidence, that claim 1 is unpatentable under 35 U.S.C. § 103(a) as obvious over Aziz and Weiss and over Aziz and Kaufman.

We have reviewed the arguments presented in the Petition and the supporting evidence regarding the obviousness of claims 2–5, the substance of which was not disputed by Patent Owner in its Response. Patent Owner, in its Response, relies solely on its arguments and evidence concerning claim 1. *See generally* PO Resp. In the Scheduling Order, we cautioned Patent Owner that any arguments for patentability not raised in the Response would be deemed waived. Paper 13, 3. In sum, we find a preponderance of the evidence establishes that claims 1–5 would have been obvious in view of Aziz and Kaufman, and in view of Aziz and Weiss.

C. Claims 6–8 as Obvious over Aziz and Rodwin

Petitioner contends that claims 6–8 would have been obvious over Aziz and Rodwin. Pet. 54–57. Patent Owner disagrees. PO Resp. 20–24.

1. Rodwin (Ex. 1008)

Rodwin describes a method for providing a remote computer with access to a local computer network. Ex. 1008, Abs. More precisely, Rodwin describes using a remote access system to authenticate a remote user, and to provide an IP address to the remote user from a dynamic IP address assignment and management server. *Id.* Figure 1A of Rodwin illustrates a remote access system, and is reproduced below:

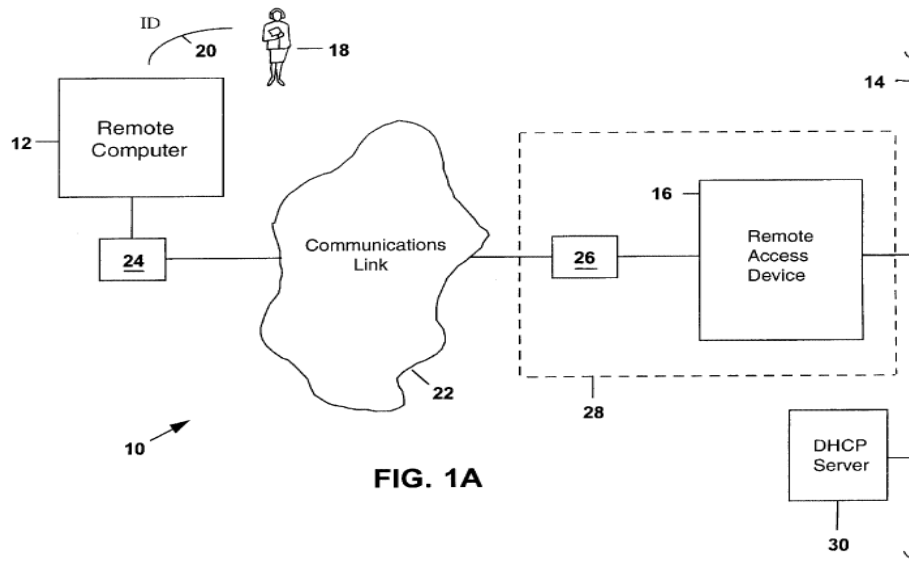


Figure 1A of Rodwin shows a simplified diagram of a remote access system in which a remote access device according to the invention provides a remote user at a remote computer with access to a local computer network. Ex. 1008, 4:18–21. As shown in Figure 1A, remote user 18 (*e.g.*, a telecommuter) *initiates an attempt to gain access to network 14 and the network services and resources available thereon, via remote access device 16 by entering username 20 into remote computer 12.* *Id.* at 1:15–35, 4:48–52. Username 20 is sent to remote access device 16 through communication link 22. *Id.* at 4:57–63. Remote access device 16 *authenticates the remote user* before the remote user is granted access to the network and network services. *Id.* at 5:16–20. Remote access device 16 also passes an identifier, which includes username 20, over network 14 to dynamic IP address assignment/management server 30. *Id.* at 5:20–23. *Server 30 dynamically assigns IP addresses based on the username.* *Id.* at Abs., 5:26–31. The IP address, which uniquely identifies the remote computer on the network, is needed by the remote computer to communicate on the network and access the network services and resources available thereon. *Id.*

2. *Analysis*

After considering the Petition, Patent Owner Response, Reply, and all evidence relied on by Petitioner and Patent Owner, we are persuaded that Petitioner has shown, by a preponderance of the evidence, that claims 6–8 would have been obvious over Aziz and Rodwin. The Petition sufficiently accounts for each of the elements in these claims and provides well-supported reasons to combine the prior art teachings to satisfy the claim elements.

Notwithstanding that Rodwin does not describe a tunneling technique to encrypt network packets expressly, Petitioner asserts that claims 6–8 are unpatentable because such a technique was known in the art as evidenced by Aziz, and that a person of ordinary skill in the art would have utilized Rodwin’s authentication approach in the firewall tunneling system of Aziz to authenticate a remote user and assign a dynamic IP address to such a user. Pet. 21–22. Indeed, Aziz describes a method for performing secure tunneling for encrypting data packets between computers and the advantages of utilizing such a method of tunneling, such as preventing hackers from discovering the data and information regarding the private network. Ex. 1005, 1:5–11, 6:3–15.

Patent Owner argues that, although Petitioner relies on Rodwin’s user authentication to teach the “authenticating the first computer” limitation recited in claim 6, “[n]owhere, however, does Petitioner explain how authenticating a user (as taught by *Rodwin*) is equivalent to authenticating a computer.” PO Resp. 20. Specifically, Patent Owner argues that Rodwin explains why usernames and passwords are an insufficient basis upon which to authenticate computers. *Id.* at 21. Patent Owner summarizes that “it is

clear that while the usernames authenticate *users*, inasmuch as the usernames are portable across devices . . . they do not authenticate *computers*.” *Id.*

Regarding the combination of Aziz and Rodwin, Patent Owner argues that Petitioner offers no compelling reasons why a person of ordinary skill in the art would ever make the combination of Aziz and Rodwin. *Id.* at 23. Patent Owner challenges Dr. Reynolds’s statement that “the system taught by Aziz would likely have been implemented in a manner that included authentication as recited in the claims,” arguing that Aziz teaches a specific methodology for authenticating users, depending on whether the user has a known IP address or a dynamically assigned IP address. . *Id.* at 23 (citing Ex. 1020 ¶ 79). Patent Owner maintains that Dr. Reynolds “never explains *why* such a combination [of Aziz and Rodwin] would ever be made.” *Id.* at 24.

Petitioner argues that Patent Owner’s Response presents no arguments apart from attorney argument already rejected by the Board. Reply 13. According to Petitioner, Patent Owner’s argument fails in that (1) authenticating users is within the Board’s construction of “authenticating”; and (2) Patent Owner provides no evidence to support its argument. *Id.* at 15. Dr. Reynolds opines that in certain network arrangements, authenticating a user validates the computer. *Id.* at 16 (citing Ex. 1028 ¶¶ 25–27); Tr. 35:17–36:7. Moreover, Dr. Nettles admits that a computer’s MAC address, such as Rodwin’s “MAC+index” mode, could be used to authenticate the computer. Reply 17; Tr. 36:17–37:11.

Claim 6 requires the step of “authenticating the first computer.” We construed the term “authenticating” to mean “a process which validates a

computer or user.” Dec. 11. Patent Owner does not propose an alternative construction for “authenticating.” The Specification does not discuss or define the term “authenticating.”

Initially, we note that based on our construction of “authenticating” — “authenticating a user or a computer” — authenticating can happen by authenticating the user, or by authenticating the computer. In this sense, looking only at the term “authenticating,” Rodwin “authenticates” because it authenticates the user. Patent Owner does not dispute that Rodwin authenticates the user. Additionally, our construction does not exclude authenticating a computer by authenticating its user. Nor, as discussed below, does Rodwin necessarily fail to authenticate the computer itself.

Nevertheless, we look at our construction of the term “authenticating” in view of how it appears in claim 6, which recites “authenticating the first computer.” Even under this approach, however, Rodwin authenticates.

First, Rodwin’s system, which Patent Owner agrees authenticates the user, is not divorced from the computer used by the user. The process of authenticating the user can also authenticate the computer. Reply 16 (citing Ex. 1028 ¶¶ 19–27). Petitioner’s expert opines that a person of ordinary skill in the art “would know that authenticating a computer and authenticating a user are interlaced concepts.” Ex. 1028 ¶ 25. In the ’891 patent, for example, Figure 11 describes the process of the user’s computer accessing the internet. Ex. 1001, 6:38–52. Step 194 of Figure 11 states “Id User Computer and Prompt for User Name and Password.” Ex. 1001, Fig. 11. Referencing Figure 11, the specification provides: “The firewall computer identifies (step 194) the computer and may prompt the user for a user name and a user password. *If the user name and password are*

authorized (step 196), the firewall updates (step 198) the tunnel records with the internet address sent as part of the connect request.” *Id.* at 6:45–50 (emphasis added). Petitioner’s expert also opines that “computers are often authenticated by implication: authenticating the user meant the computer was authenticated and trusted also.” Ex. 1028 ¶ 25. We credit this testimony; we are not persuaded by Patent Owner’s argument that the process of authenticating Rodwin’s user excludes authenticating the computer being used by the user.

Second, Petitioner argues that the MAC+index mode of Rodwin can be used to authenticate the computer. Reply 16–17 (citing Ex. 1028 ¶¶ 28–34). Petitioner argues that this point, raised for the first time in its Reply Brief, is properly responsive to Patent Owner’s arguments regarding the teachings of Rodwin. Tr. 44:17–45:7. We agree. Patent Owner argues in its Response that Rodwin authenticates users, using usernames, but that Rodwin’s usernames do not authenticate computers. PO Resp. 20–22. Both Patent Owner’s expert and Petitioner’s expert weighed in on this argument. Ex. 1027, 85:9–16; Ex. 1028 ¶¶ 25–34. Patent Owner addressed the MAC+index approach in its Motion for Observations on Cross-Examination. Paper 35, 4. Patent Owner also discussed the MAC address issue at oral hearing, agreeing that a “MAC address will authenticate a computer” while maintaining the position that “MAC addresses simply are not sufficient.” Tr. 64:24–66:15. Thus, we consider this argument as properly before us.

Regarding the merits of this argument, we are persuaded that Rodwin “authenticates” computers through use of their MAC address. Rodwin, like Aziz, has a DHCP server that assigns IP addresses to computers. Ex. 1008, 10:4–12. Rodwin provides that it is desirable that each remote computer “be

uniquely and deterministically identifiable by the dynamic IP address assignment/management server(s).” *Id.* at 2:39–40. The MAC+index mode of Rodwin identifies a mode of operation of the remote access device in which the reconnection feature does not work but username sharing is allowed. *Id.* at 9:13–16. Petitioner’s expert opines that one of ordinary skill in the art would have been aware of the automated use of addresses such as MAC addresses as a method for automatically authenticating a computer. Ex. 1028 ¶¶ 31 (citing Ex. 1007, 183), 33. Patent Owner’s expert agrees that a DHCP server “could use the computer’s MAC address, determine whether that MAC address is on an approved list of computers and, if it is on that approved list of computers, to return an IP address.” Reply 17 (citing Ex. 1027, 85:9–16). Rodwin, in addition to authenticating a user, also provides for authenticating a computer.

Regarding the combination of Aziz and Rodwin, Petitioner argues that a person of ordinary skill in the art “would have combined Aziz with Rodwin, using Rodwin’s authentication approach to create a new firewall-to-firewall tunnel as taught in Aziz.” Pet. 21. Petitioner further explains that Rodwin’s “remote access point could readily and predictably have been coupled to the Aziz firewall to provide multiple users of the single remote access point the enhanced security of the Aziz firewall-to-firewall tunneling scheme.” *Id.* at 21–22 (citing Ex. 1020 ¶¶ 79–80). Dr. Reynolds testifies that, in the combined system, the remote access device of Rodwin would support remote users with changing IP addresses and Aziz’s tunnel would provide secure communication between the remote users and the network served by the remote access device. Ex. 1020 ¶ 80. We also credit the testimony of Dr. Reynolds that combining the teachings of Aziz and Rodwin

would not have been beyond the skill level of one of ordinary skill in the art, and would have yielded nothing more than predictable results. Ex. 1028 ¶¶ 19–23.

Patent Owner’s argument, which focuses narrowly on an exemplary network of Aziz that utilizes two firewall servers on two different networks (FWX and FWY), does not account for Aziz’s disclosure that its tunneling technique may be implemented in different network configurations. See Ex. 1005, Fig. 8. Rodwin’s network configuration involves only one network and the server is connected to that network (item 14 of Figure 1A of Rodwin, reproduced above). Notwithstanding paragraph 32 of its expert’s declaration (Ex. 2002), Patent Owner provides no persuasive explanation as to why a person of ordinary skill in the art could not have applied Aziz’s tunneling technique to a communication between a remote computer and a local network as disclosed in Rodwin, given all of the stated security advantages of the tunneling technique and teachings of exemplary implementations in Aziz.

Upon review of the complete record, we find that Petitioner has established, by a preponderance of the evidence, that claim 6 is unpatentable under 35 U.S.C. § 103(a) as obvious over Aziz and Rodwin. We have reviewed the arguments presented in the Petition and the supporting evidence regarding the obviousness of claims 7 and 8, the substance of which was not disputed by Patent Owner in its Response. Patent Owner, in its Response, relies solely on its arguments and evidence concerning claim 6. See *generally* PO Resp. In the Scheduling Order, we cautioned Patent Owner that any arguments for patentability not raised in the Response would be deemed waived. Paper 13, 3. In sum, we find a preponderance of the

evidence establishes that claims 6–8 would have been obvious in view of Aziz and Rodwin.

D. Conclusion

For the foregoing reasons, after considering the Petition, Patent Owner Response, Reply, and all evidence relied upon by Petitioner and Patent Owner, we are persuaded that Petitioner has shown, by a preponderance of the evidence, that claims 1–5 would have been obvious over Aziz and Kaufman and over Aziz and Weiss, and that claims 6–8 would have been obvious over Aziz and Rodwin.

III. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–8 of the '891 patent are held unpatentable;
and

FURTHER ORDERED that because this is a final written decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2014-01216
Patent 5,825,891

For PETITIONER:

Donald Daybell
d2dptabdocket@orrick.com

Bas de Blank
M2BPTABDocket@orrick.com

Monte M.F. Cooper
M26PTABDocket@orrick.com

Jason Yu
J2YPTABDocket@orrick.com

For PATENT OWNER:

Tarek Fahmi
tarek.fahmi@ascendalaw.com