Trials@uspto.gov
571-272-7822

Paper 8
Entered: 16 May 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ORACLE CORPORATION
Petitioners,

v.

CLOUDING IP, LLC
Patent Owner.

Case IPR2013-00100 (JL)
Patent 5,825,891

Before JAMESON LEE, JONI Y. CHANG, and MICHAEL W. KIM, *Administrative Patent Judges*.

CHANG, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Oracle Corporation ("Oracle") filed a petition requesting an *inter partes* review of claims 1-8 of U.S. Patent 5,825,891 (Ex. 1001, "the '891 patent"). (Paper 1, "Pet.") In response, Clouding IP, LLC ("Clouding") filed a patent owner preliminary response. (Paper 7, "Prel. Resp.") We have jurisdiction under 35 U.S.C. § 314.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a) which provides as follows:

> THRESHOLD -- The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

Upon consideration of the petition and patent owner preliminary response, we determine that the information presented in the petition establishes that there is a reasonable likelihood that Oracle would prevail with respect to claims 1-8 of the '891 patent. Accordingly, pursuant to 35 U.S.C. § 314, we authorize an *inter partes* review to be instituted as to claims 1-8 of the '891 patent.

A. Related Proceedings

Oracle indicates that the '891 patent is involved in co-pending litigation captioned *Clouding IP, LLC v. Oracle Corp.*, Case No. 1:12-cv-00642 (D.Del.). (Pet. 4.)

B. The ’891 Patent and Illustrative Claims

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.)

Of the challenged claims, claims 1 and 6 are independent claims. As to the dependent claims, claims 2-5 depend from claim 1, and claims 7 and 8 directly or indirectly depend from claim 6. Claims 1 and 6 are illustrative for purposes of this decision, and are reproduced as follows:

> 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.
>
> 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.

C. Prior Art Relied Upon

Oracle relies upon the following prior art references:

Aziz	U.S. Patent 5,416,842	May. 16, 1995	(Ex. 1002)
Rodwin	U.S. Patent 5,812,819	Sep. 22, 1998	(Ex. 1003)

Stallings et al., *Network and Internetwork Security*, Prentice Hall, 1995 (Ex. 1005)

Kaufman et al., *Network Security: Private Communication in a Public World,* Prentice-Hall, 1995 (Ex. 1006)

D. The Asserted Grounds

Oracle alleges that the challenged claims are unpatentable based on the following grounds:

1. Claims 1-5 are unpatentable under 35 U.S.C. § 103(a) over Aziz and Stalling;
2. Claims 1-5 are unpatentable under 35 U.S.C. § 103(a) over Aziz and Kaufman;
3. Claims 6-8 are unpatentable under 35 U.S.C. § 103(a) over Aziz and Rodwin;
4. Claims 6-8 are unpatentable under 35 U.S.C. § 103(a) over Aziz and Stallings; and
5. Claims 6-8 are unpatentable under 35 U.S.C. § 103(a) over Aziz and Kaufman.

II. ANALYSIS

A. Claim Construction

As a first step in our analysis for determining whether to institute a review, we determine the meaning of the claims. In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b). Under the broadest reasonable construction standard, claim terms are presumed to be given their ordinary and customary meaning as would be understood by one of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). An inventor may rebut that presumption by providing a definition of the term in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). Here, the parties have not alleged that the inventor of the '891 patent acted as his own lexicographer and gave any claim term a special definition different from its recognized meaning to one with ordinary skill. Therefore, the words of the claim will be given their plain meaning unless the plain meaning is inconsistent with the specification. *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989). In that regard, we must be careful not to read a particular embodiment appearing in the written description into the claim if the claim language is broader than the embodiment. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Oracle provides its interpretations for three claim terms, "temporary configuration password," "authenticating," and "tunnel record information." (Pet. 16-18.) Clouding also proposes interpretations for those claim terms and for the claim term "tunnel record." For this decision, we will construe each of the

claim terms identified by the parties in turn.

1. "Temporary configuration password" (Claim 1)

The claim term "temporary configuration password" appears only in the following limitations of claim 1 (emphasis added):

> 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;

Clouding contends that the term means "a transitory password used when establishing tunnels for secure communication between computers." (Prel. Resp. 6.) We do not agree with that claim construction. At the outset, Clouding does not allege that the specification provides a special definition to support its contention, and we did not find one. We further observe that the term "transitory" is vague and it would not be meaningful to use a key claim word ("password") in the claim construction. Moreover, Clouding's proposed construction seems to import a limitation from the specification into the claim, namely "used when establishing tunnels for secure communication between computers," and does not provide sufficient relationship between the words "configuration" and "password."

On the other hand, Oracle interprets the claim term "temporary configuration password" to include "non-permanent codes which are used in connection with a configuration process." (Pet. 16.) That construction stays closer to the claim language without using one of the key words. *Renishaw PLC v. Marposs Societa per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998) (The construction that stays true

to the claim language and most naturally aligns with the inventor's description is likely to be the correct construction.) However, we find it necessary to clarify further the term "non-permanent codes." As ordinarily understood, "temporary" means "lasting or effective for a time only; not permanent" and "password" means "a string of characters typed into a computer to identify and obtain access for an authorized user."[1]

We next review the specification of the '891 patent as part of our claim construction analysis. *See Phillips*, 415 F.3d at 1317 (The specification is the single best guide to the meaning of a claim term.). Figure 10 depicts a flow chart for generating tunnel record using a password and is reproduced as follows:

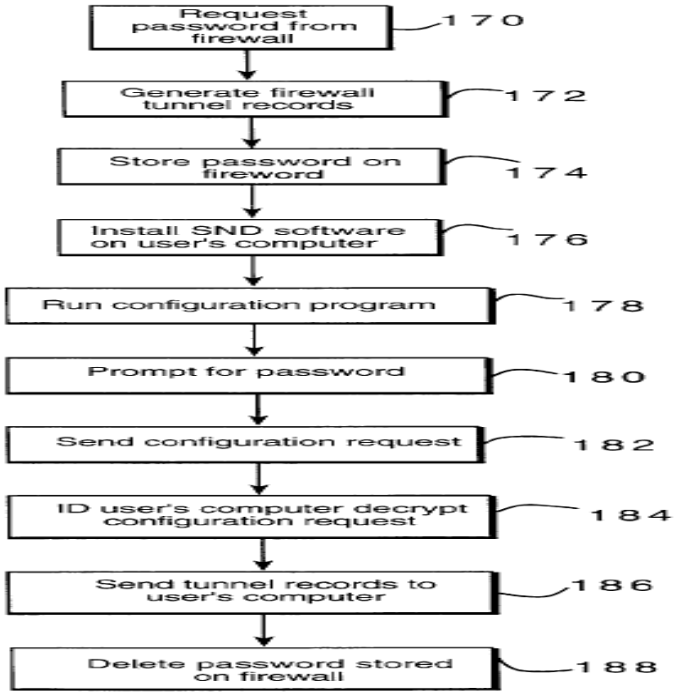


FIG. 10

[1] *See e.g., Random House Webster's College Dictionary* (2nd ed. 1999).

Directing our attention to the following portions of the specification, Oracle indicates that claims 1-5 are related to the embodiment illustrated in Figure 10 of the '891 patent (Ex. 1001, 6:5-37, emphasis added):

> Typical users have non-firewall computers and may wish to transfer encapsulated/encrypted data with a firewall computer. To avoid requiring that a typical user generate tunnel records and instead of having a separate trusted computer provide secret keys to two computers, a firewall computer 16, 18 may provide secret keys to other computers.
>
> Referring also to FIG. 10, when a user wishes to transfer packets between his/her computer and a firewall computer, the user requests (step 170) a *password (a onetime pad)* from the firewall operator. The operator then generates (step 172) tunnel records for each tunnel over which the user's computer and the firewall computer may transfer network packets. The operator also stores (step 174) *the password* given to the user on the firewall computer. The user installs (step 176) the security network driver (SND) software on his/her computer and runs (step 178) a *configuration program*. The configuration program prompts (step 180) the user for *the password* and sends (step 182) a configuration request to the firewall computer.
>
> The firewall computer identifies (step 184) the user's computer as the sender of the request and notifies the user's computer of the available tunnels by sending (step 186) the complete tunnel records, including secret keys, associated with each tunnel to the user's computer. The tunnel records are sent through network packets that are encrypted using the password and the encryption algorithm. Afterwards, *the firewall deletes (step 188) the password*, and further network packets are transmitted between the two computers through the available tunnels and encrypted according to the secret key associated with each tunnel.

In the light of the specification, we construe broadly, but reasonably, the claim term "temporary configuration password" as "non-permanent codes to

identify an authorized user, which are used in connection with an initialization process to enable the user to access a secured network."

2. "Authenticating" (Claims 6, 7, and 8)

The claim term "authenticating" is recited in the following claim limitations: "*authenticating* the first computer" (claim 6), "wherein *authenticating* includes: identifying the first computer" (claim 7), "wherein *authenticating* further includes: prompting the first computer for an authorization code" (claim 8). In the context of network communication, the word "authentication" ordinarily means "the process by which the system validates a user's logon information." [2]

Oracle asserts that the claim term "authenticating" should be interpreted as including "any process which uniquely identifies the device or user in question" (Pet. 18), whereas Clouding urges that the claim term means "establishing authenticity, or establishing as valid" (Prel. Resp. 7). To reconcile those proposed constructions, we turn to the specification of the '891 patent.

While the specification does not use the term "authenticating," Oracle indicates that claims 6-8 are related to the embodiment illustrated in Figure 11 of the '891 patent, which is reproduced as follows:

[2] *See e.g., Microsoft Computer Dictionary*, Microsoft Press, 5th edition, 2002.

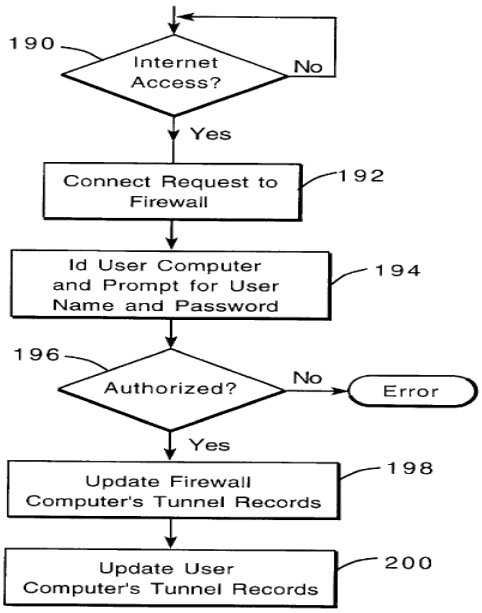


FIG. 11

Referencing Figure 11, the specification provides the following descriptions (Ex. 1001, 6:37-52, emphasis added):

> Referring to FIG. 11, generally, each time the user's computer accesses (step 190) the internet, a new internet address is assigned. The firewall computer needs to know the new address in order to update the tunnel records. To notify the firewall computer of the new internet address, each time the user's computer accesses the internet, the configuration software issues (step 192) a connect request to the firewall computer. 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. The configuration software also updates (step 200) the non-firewall computer's tunnel records with the computer's new internet address.

In the light of the specification of the '891 patent, we construe the claim term "authenticating" as "a process which validates a computer or user."

3. "Tunnel record" (Claim 6)

The claim term "tunnel record" by itself without the word "information" appears only in claim 6 which recites "updating a *tunnel record* corresponding to the connection request with the first computer's *network address*" (emphasis added). Clouding asserts that the claim term "tunnel record" should be construed as "a *record concerning tunnels* for secure communications between computers." (Prel. Resp. 6-7, emphasis added.) While that proposed construction may provide a context of using a tunnel record in relation of secure communication between computers, we find it necessary to ascertain the meaning of the claim term in light of the specification.

The specification of the '891 patent provides that "operators of the two computers may verbally exchange a secret key for each tunnel between the computers and then manually initialize the computer to transfer data by generating a *tunnel record including a secret key* for each tunnel between the two computers" (Ex. 1001, 5:66-6:3, emphasis added); "the firewall updates (step 198) *the tunnel records with the internet address* sent as part of the connect request" (Ex. 1001, 6:47-50, emphasis added); and the "configuration software also updates (step 200) the non-firewall computer's *tunnel records with the computer's new internet address*" (Ex. 1001, 6:50-52, emphasis added).

In the context of the specification, we construe the claim term "tunnel record" as information including a key for a tunnel or a network address of a computer that will be using the tunnel.

4. "Tunnel record information" (Claims 1, 2, and 3)

The claim term "tunnel record information" is recited, for example, in the limitation of claim 3 "after receiving *the tunnel record information* from the second computer, sending a network packet over the network through a virtual tunnel, the network packet being encrypted in accordance with the secret tunnel encryption key in *the tunnel record information* corresponding to the virtual tunnel." (Emphasis added).

Clouding asserts that the claim term "tunnel record information" should be construed as "*information* associated with a *tunnel record*." (Prel. Resp. 7, emphasis added.) We observe that it is not meaningful to use the claim term to define itself.

As Oracle points out, the specification of the '891 patent provides that "[a] tunnel record corresponding to the connection request with the first computer's *network address* is then updated" and "[h]aving a firewall computer provide tunnel records, including *secret keys*, eliminates the need for a separate 'trusted computer.'" (Pet. 18, citing to Ex. 1001, 2:18-20, 2:27-29, emphasis added.) Upon consideration of the specification, we agree with Oracle's claim construction, and interpret the claim term "tunnel record information" as any portion of a tunnel record, such as encryption information (*e.g.*, a key) or a network address.

B. Claims 1-5 – Unpatentable Over Aziz and Kaufman

Oracle asserts that claims 1-5 are unpatentable under 35 U.S.C. § 103(a) as obvious over Aziz and Kaufman. (Pet. 25-29.) As support, Oracle provides detailed explanations as to how each claim limitation is met by the cited references, and a declaration of Dr. Paul F. Reynolds[3] ("Dr. Reynolds"). (*Id*., citing to Ex. 1004, ¶¶ 31-36.) Upon review of Oracle's analysis and supporting evidence, we determine that Oracle's assertion has merit.

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966).

[3] Dr. Reynolds has a Ph.D. in computer science and extensive experience in distributed computing and simulation. (Ex. 1004, ¶¶ 1-11.) As such, we conclude that Dr. Reynolds is qualified to testify as to the understanding of a person of ordinary skill one skill in the art.

Kaufman

Kaufman describes a network authentication scheme, specifically a technique for distributing keys in a secure manner. (Ex. 1006, 266-269.[4]) Figure 10-1 of Kaufman, reproduced below, illustrates Kaufman's key distribution technique (Ex. 1006, 269):

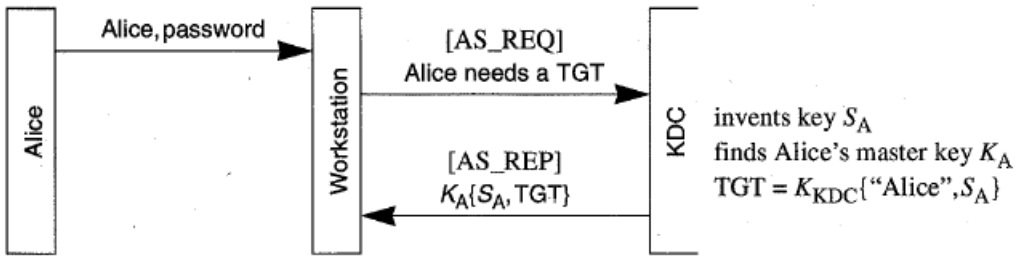


Figure 10-1. Obtaining a TGT

As shown in Figure 10-1 of Kaufman, Alice (a user) logs into the workstation by entering *her name and password*. (Ex. 1006, 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. (Ex. 1006, 267.) After that, the workstation *forgets* Alice's password and only remember S_A and the TGT. (*Id*.)

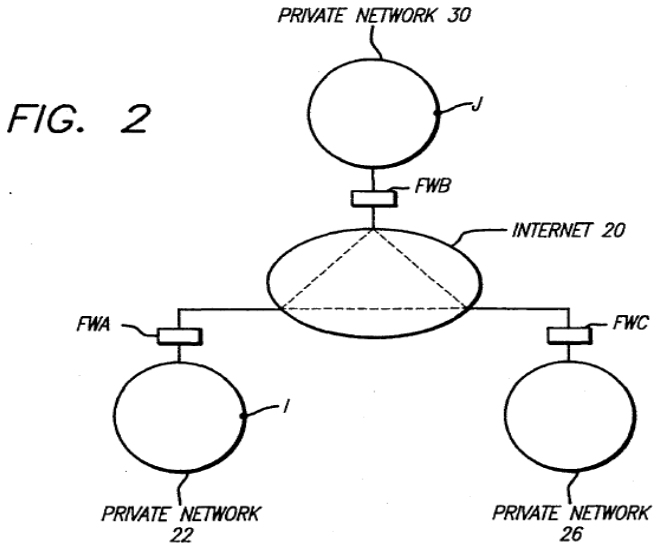
[4] The page numbers in our citation to Kaufman are the original page numbers in the textbook, on the top right and left corners of each page.

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*.)

Aziz

In the petition, rather than relying upon Kaufman to disclose a tunneling technique to encrypt network packets, Oracle cites Aziz for such a teaching. Specifically, Aziz describes a method to perform secure *tunneling* for encrypting data packets between computers. (Ex. 1002, 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 to be discovered by a hacker. (*Id*.) When transmitting an IP packet using tunneling, all an unintended observer can determine is that there are 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 bases 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 an Internet 20 coupled to a private network 22 through a firewall server FWA:



As shown in Figure 2 of Aziz, each private network (22, 26, and 30) is coupled through a firewall server (FWA, FWC, and FWB, respectively) to the Internet 20. (Ex. 1002, 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 the Internet 20. For example, when a node I on private network 22 sends a packet to a node J on private network 30, the firewall server FWA first determines that node J is coupled to network 30, and that firewall server FWB serves network 30. (Ex. 1002, 5:54-6:2.) Then, the firewall server FWA encapsulates the original IP data packet (header and data) and transmits the data packet in an encrypted IP packet intended for the remote firewall FWB. (*Id*.)

In another embodiment, Aziz describes a portable computer that connects to a public network where the computer dynamically is assigned an IP address. (Ex. 1002, 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*.)

Rationale to combine the prior art references

In its preliminary response, Clouding does not dispute that the cited prior art collectively describes all of the claim limitations of claims 1-5. Rather, Clouding argues that a person of ordinary skill in the art at the time of the invention would not have combined the teachings of Aziz and Kaufman. (Prel. Resp. 16-18.) In particular, Clouding argues that "adding [an] extra layer of encrypted communication within a protected network (behind the firewall) would not serve to further secure the communications from the source to the destination and would only add needless complexity to an already complicated system." (Prel. Resp. 16.) Clouding contends that the proposed combination of Aziz and Kaufman "ignores the actual teachings of Aziz" which already discloses passing keys between computers in an encrypted fashion. (Pre. Resp. 17.) Clouding further alleges that Oracle fails to explain why a person of ordinary skill in the art would abandon the key distribution teachings of Aziz and adopt Kaufman's key distribution scheme. (*Id*.)

We are not persuaded by Clouding's arguments. Clouding does not provide a sufficient explanation or credible evidence to support that combining the firewall tunneling system of Aziz with Kaufman's key distribution technique is beyond the skill level of a person of ordinarily skill in the art, or that the combination of elements as claimed yields more than predictable results.

We first note that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416. In that regard, the Court has recognized that "when a patent claims a structure already known in the prior art that is altered by

the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *Id*. "The obviousness analysis cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation, or by overemphasis on the importance of published articles and the explicit content of issued patents." *Id.* at 419. A prior art reference must be considered for everything it teaches by way of technology and is not limited to the particular invention it is describing and attempting to protect. *EWP Corp. v. Reliance Universal Inc*., 755 F.2d 898, 907 (Fed. Cir.), *cert. denied*, 474 U.S. 843 (1985).

Here, Clouding's arguments narrowly focus on Aziz's disclosure of a communication between a node I and firewall FWA *within a protected network, behind the firewall* (shown in Figure 2 of Aziz). (Prel. Resp. 16-17.) We note that Aziz expressly explains that the network topology illustrated in Figure 2 is *representative* and that a person of ordinary skill in the art could have implemented Aziz's tunneling technique in other network arrangements. (*See e.g.*, Ex. 1002, 5:11-16, 10:37-11:53, 11:55-12:11.) In fact, Aziz illustrates another exemplary implementation of its tunneling technique that involves a portable computer connected to a public network (*outside the firewall*). (Ex. 1002, 10:37-11:53, Fig. 8.) Clouding fails to explain why one of ordinary skill in the art would not have applied Aziz's tunneling technique to a network in which a computer initiates a communication *outside the firewall*, such as Kaufman's communication connection between Alice and the KDC, in light of Aziz's disclosure given all of the stated security advantages of the tunneling technique and teachings of exemplary implementations.

In any event, Oracle articulates that a person of ordinary skill in the art "would have considered the use of Kaufman's key distribution technique in the firewall tunneling system of Aziz to have been predictable and desirable at the time of filing." (Pet. 25.) Oracle also explains that "the key distribution technique described by Kaufman. . . could readily and predictably have been implemented to establish the Aziz firewall tunnel to provide enhanced security." (*Id*.)

In that regard, Oracle's expert, Dr. Reynolds, testifies (Ex. 1004, ¶ 35, emphasis added):

> *The combined system of Aziz and Kaufman would result in the use of a password shared between the tunnel endpoints and used once to encrypt/decrypt a tunnel record.* Subsequent communication between the tunnel endpoints would use the key transmitted in the tunnel record. The combined system would not use Aziz's public key technology, but would instead use the session key (the analog of the key in the tunnel record) generated on the second computer (the analog of the KDC in Kaufman Fig. 10-1). In the combined system, the second computer (analogous to the KDC in Kaufman's Fig. 10-1) generates a new password along with the other tunnel parameters, and sends the tunnel record to the first computer encrypted with the master key shared by the two computers. *The substitution of one well-known authentication and key distribution scheme for another well-known scheme would have been within the realm of ordinary skill at the time of filing.*

On this record, we credit the testimony of Dr. Reynolds that the combined system would result in the use of a password shared between the tunnel endpoints and used once to encrypt and decrypt a tunnel record, and the mere substitution of Kaufman's authentication and key distribution scheme for Aziz's public key distribution scheme predictably uses prior art elements according to their

established function. For the foregoing reasons, we determine that Oracle has demonstrated that there is a reasonable likelihood that it would prevail with respect to claims 1-5 based on the grounds that these claims are obvious over Aziz and Kaufman.

Other considerations

Clouding urges the Board not to institute an *inter partes* review pursuant to 35 U.S.C. § 325(d). (Prel. Resp. 24-25.) According to Clouding, the subject matter of Oracle's proposed combination of Aziz and Kaufman was considered by the Office during the original prosecution of the '891 patent. (*Id*.) More specifically, Clouding alleges that, in the original prosecution, the examiner had considered Aziz and *Kerberos Network Authentication Service (V5)*, which describes an earlier version of the same network authentication protocol as Kaufman. (*Id*.)

Section 325(d) of Title 35 of the United States Code does not require the Director, in deciding whether to institute *inter partes* review, to defer to a prior determination in the Office, even one which considered the same prior art and arguments. The statute gives the Director the authority not to institute a review on the basis that the same or substantially the same prior art or arguments were presented previously to the Office, but does not require that result.

Here, unlike the case in *ex parte* prosecution of the application that issued as the '891 patent, Oracle is a party to the proceeding. Oracle presents different arguments and new supporting evidence that were not before the examiner, shedding a different light on Aziz and Kaufman. As such, we decline to deny this

ground of unpatentability based on the combination of Aziz and Kaufman under 35 U.S.C. § 325(d).

C. Claims 6-8 – Unpatentable Over Aziz and Rodwin

Oracle asserts that claims 6-8 are unpatentable under 35 U.S.C. § 103(a) over Aziz and Rodwin. (Pet. 30-36.) We have reviewed Oracle's analysis and supporting evidence, and determine that Oracle's assertion has merit.

Rodwin describes a method for providing a remote computer with access to a local computer network. (Ex. 1003, 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 as follows:

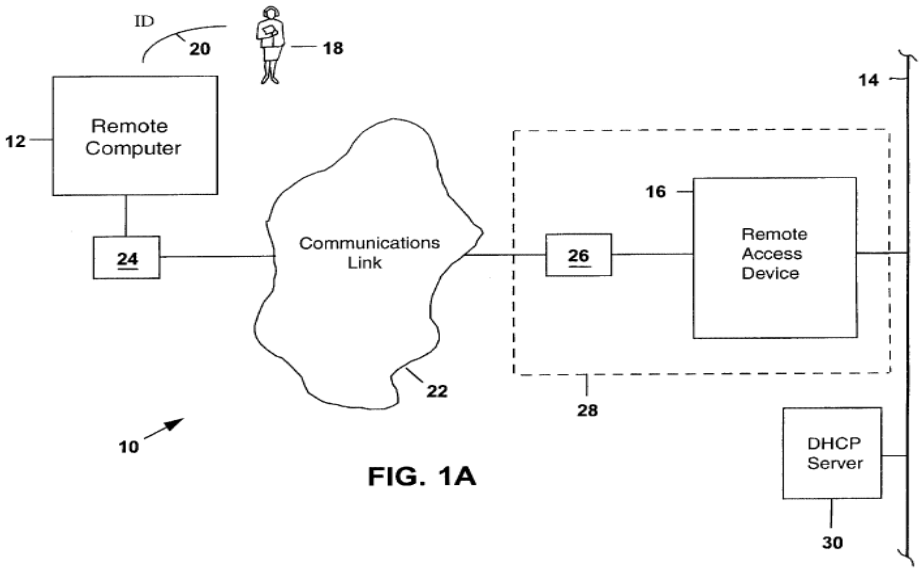


FIG. 1A

As shown in Figure 1A of Rodwin, a remote user 18 (*e.g.*, a telecommuter) *initiates an attempt to gain access to the network* 14 and the network services and resources available thereon, via the *remote access device 16 by entering a username 20* into the remote computer 12. (Ex. 1003, 1:15-35, 4:48-52.) The username 20 is sent to the remote access device 16 through the communication link 22. (Ex. 1003, 4:57-63.) The remote access device 16 *authenticates the remote user* before the remote user is granted access to the network and network services. (Ex. 1003, 5:16-20.) The remote access device 16 also passes an identifier, which includes the username 20, over the network 14 to a dynamic IP address assignment/management server 30. (Ex. 1003, 5:20-23.) The *server 30 dynamically assigns IP addresses based on the username*. (Ex. 1003, Abs., 5:26-31.) The IP address uniquely identifies the remote computer on the network, and it is needed by the remote computer to communicate on the network and access the network services and resources available thereon. (*Id*.)

Notwithstanding that Rodwin does not describe a tunneling technique to encrypt network packets expressly, Oracle 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. 30-31.) Indeed, as we discussed previously, Aziz describes a method for performing secure tunneling for encrypting data packets between computers, and the advantages to utilizing such a method of tunneling, such as preventing hackers from discovering the data and information regarding the private network. (Ex. 1002, 1:5-11, 6:3-15.)

In its preliminary response, Clouding likewise does not dispute that the combination of the prior art references relied upon by Oracle collectively describes all of the claim limitations of claims 6-8. Rather, Clouding counters that Oracle presents "no reason why a person of ordinary skill in the art would abandon the teachings of Aziz to adopt contrary teachings of Rodwin concerning the storing of address mappings." (Prel. Resp. 19-20.) To support its contention, Clouding points out that Aziz indicates that "when a mobile computer with a [Dynamic Host Configuration Protocol (DHCP)] assigned IP address is involved, the only mappings required are those at a remote firewall computer and not at the firewall computer to which the 'client' connects." (Prel. Resp. 19-20, citing to Ex. 1002, 11:39-46.)

Clouding's argument is misplaced, as it focuses narrowly on an exemplary network of Aziz that utilizes *two firewall servers on two different networks* (FWX and FWY, Ex. 1002, Fig. 8). As discussed above, Aziz's tunneling technique may be implemented in different network configurations. Clouding fails to recognize that 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).

Clouding provides no 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, in light of Aziz's disclosure given all of the stated security advantages of the tunneling technique and teachings of exemplary implementations. Clouding also does not provide a sufficient explanation or credible evidence to support that combining the firewall tunneling system of Aziz with Rodwin's authentication approach is beyond the

skill level of a person of ordinarily skill in the art, or that the combination of elements as claimed yields more than predictable results.

In any event, Oracle articulates that a person of ordinary skill in the art "would have considered the use of Rodwin's authentication approach in the firewall tunneling system of Aziz to have been predictable and desirable at the time of filing." (Pet. 30.) Oracle 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." (Pet. 30-31, citing to Ex. 1004, ¶¶ 37-42.) Dr. Reynolds also 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. 1004, ¶ 40.)

On this record, we determine that Oracle's articulated rationale to combine Rodwin's authentication approach with the tunneling technique of Aziz is persuasive. Accordingly, Oracle has demonstrated that there is a reasonable likelihood that it would prevail with respect to claims 6-8 based on the ground that these claims are unpatentable over Aziz and Rodwin.

D. Other Asserted Grounds

Oracle also asserts that claims 1-8 are unpatentable over Aziz and Stallings, and claims 6-8 are unpatentable over Aziz and Kaufman. (Pet. 19-24, 37-43.) Those asserted grounds are denied as redundant in light of the determination that there is a reasonable likelihood that the challenged claims are unpatentable based

on the grounds of unpatentability on which we institute an *inter partes* review. *See* 37 C.F.R. § 42.108(a).

III. CONCLUSION

For the forgoing reasons, we determine that the information presented in the petition establishes that there is a reasonable likelihood that Oracle would prevail with respect to claims 1-8 of the patent '891.

IV. ORDER

Accordingly, it is

ORDERED that pursuant to 35 U.S.C. § 314, an *inter partes* review is hereby instituted as to claims 1-8 of the '891 patent for the following grounds:

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

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(d) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial is commencing on the entry date of this decision; and

FURTHER ORDERED that an initial conference call with the Board is scheduled for 3:00 PM Eastern Time on May 30, 2013; the parties are directed to the Office Trial Practice Guide[5] for guidance in preparing for the initial conference

[5] *Office Patent Trial Practice Guide*, 77 *Fed. Reg*. 48756, 48765-66 (Aug. 14, 2012).

call, and should come prepared to discuss any proposed changes to the Scheduling Order entered herewith and any motions the parties anticipate filing during the trial.

For PETITIONER:

Greg Gardella
Scott A. McKeown
OBLON SPIVAK
cpdocketgardella@oblon.com
cpdocketmckeown@oblon.com

For PATENT OWNER

Tarek N. Fahmi
Amy J. Embert
Fahmi, Sellers & Embert
tarek.fahmi@fseip.com
amy.embert@fseip.com