

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

Case IPR2019-00825
Patent 9,762,397 B2

Before SALLY C. MEDLEY, KAMRAN JIVANI, and
JOHN D. HAMANN, *Administrative Patent Judges*.

MEDLEY, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition for *inter partes* review of claims 1 and 2 of U.S. Patent No. 9,762,397 B2 (Ex. 1001, “the ’397 patent”). Paper 2 (“Pet.”). MPH Technologies Oy, (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). Institution of an *inter partes* review is authorized by statute when “the information presented in the petition . . . and any response . . . 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.” 35 U.S.C. § 314(a). Upon consideration of the Petition and Preliminary Response, we decline to institute review of claims 1 and 2 of the ’397 patent.

A. Related Matters

Petitioner and Patent Owner indicate that the ’397 patent is the subject of the following currently pending court proceeding: *MPH Techs. Oy v. Apple Inc.*, Case No. 4:18-cv-05935-PJH (N.D. Cal.). Pet. 2; Paper 4, 1. The parties also identify the following proceedings involving different, but related patents: IPR2019-00822, IPR2019-00823, IPR2019-00824, and IPR2019-00826. *Id.*

B. The ’397 Patent

The Specification of the ’397 patent describes a method and system for enabling secure forwarding of a message from a first computer to a second computer via an intermediate computer. Ex. 1001, code (57). The first computer forms a secure message by giving the message a unique identity and a destination address. *Id.* The message is sent from the first computer to the intermediate computer. *Id.* The intermediate computer uses the destination address and the unique identity to find an address to the

second computer. *Id.* The destination address is substituted with the found address to the second computer and the unique identity is substituted with another unique identity. *Id.* The message is then forwarded to the second computer. *Id.*

“An example of a telecommunication network of the invention is illustrated” per Figure 1, reproduced below. *Id.* at 9:65–66.

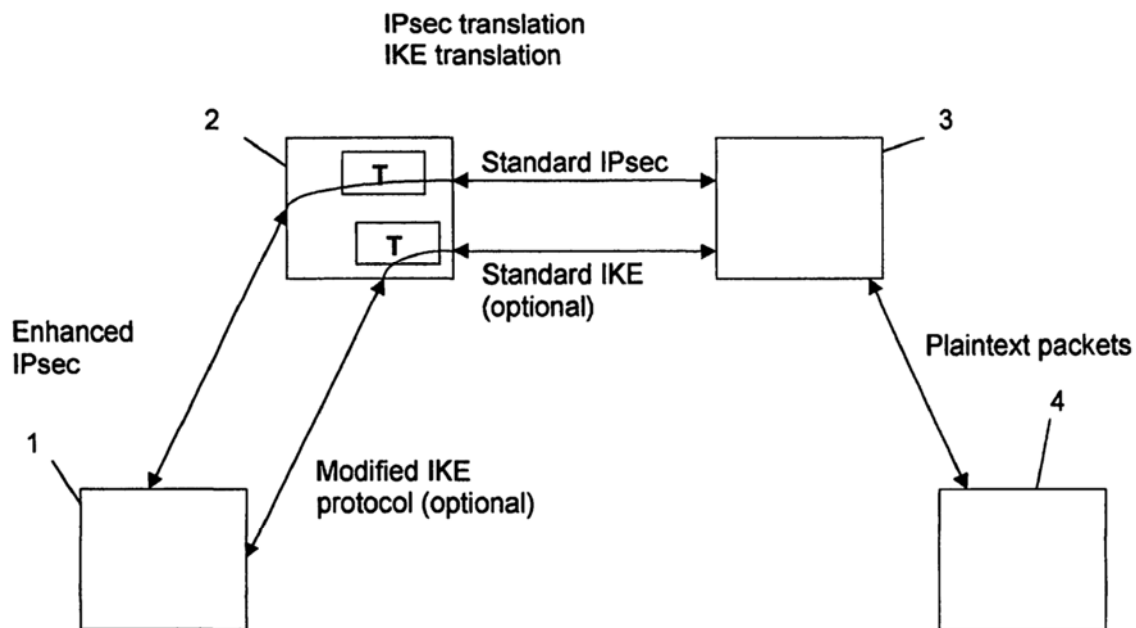


FIG. 1

Figure 1 is an illustration of a telecommunication network, where a client computer 1 is served by intermediate computer (server 2) and host computer 4 is served by a second computer (security gateway 3). *Id.* at 9:65–10:3. Security gateway 3 supports the standard IP security protocol (IPsec) and optionally the Internet Key Exchange (IKE) protocol. *Id.* at 10:3–4. Client computer 1 and server 2 support a modified IPsec and IKE protocol. *Id.* at 10:5–6. In particular, an IPsec connection is formed between client

computer 1 and security gateway 3 by forming a security association (SA) between the computers with a preceding key exchange. *Id.* at 10:40–45. A security association is uniquely identified by three parameters. *Id.* at 2:35–36. The first parameter is a Security Parameters Index (SPI) which is carried in AH (Authentication Header) and ESP (Encapsulating Security Payload) headers. *Id.* at 2:36–38. The second parameter is an IP destination address, which is the address of the destination end point of the SA, and the third parameter is a security protocol identifier, which identifies whether the association is an AH or ESP security association. *Id.* at 2:40–45.

The key exchange between first and second computer takes place manually or with an automatic key exchange protocol such as the IKE protocol. *Id.* at 10:45–48. The key exchange is performed using a standard IKE protocol between server 2 and security gateway 3, and a modified IKE protocol is used between client computer 1 and server 2. *Id.* at 10:48–51. Messages to be sent to host terminal 4 from client computer 1 are first sent to server 2, wherein an IPsec translation and an IKE translation takes place. *Id.* at 10:54–56. The message is then sent to security gateway 3, which sends the message in plain text to host terminal 4. *Id.* at 10:56–58.

Figure 3, reproduced below, illustrates an example of an IPsec translation table used by the intermediate computer to change the outer IP address and SPI value. *Id.* at 9:52–54.

c-addr-1	c-addr-2	c-SPI-1	c-SPI-2	s-addr-2	s-addr-3	s-SPI-2	s-SPI-3
195.1.2.3	212.90.65.1	0x80000001	0x12341234	212.90.65.1	103.6.5.4	0x1230012	0x56785678
...	...	...	...	...	...	...	...

Figure 3 shows a partitioned translation table, where the left side, identified by the prefix c-, refers to the network connection between the first computer and an intermediate computer, and the right side, identified by the prefix s-, refers to the network connection between the intermediate

computer and a second computer. *Id.* at 11:33–42. The postfix number (-1, -2, or -3) identifies the host in question. *Id.* at 11:42–43. When the intermediate computer receives the packet sent, it performs an address and SPI translation, ensuring that the security gateway (host 3 of Figure 1) can accept the packet. *Id.* at 11:63–66. The intermediate computer does not have cryptographic keys to undo the IPsec processing done by the mobile terminal, and cannot decrypt the packet, but is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer. *Id.* at 11:67–12:6. Thus, in this example, SPI is changed to 0x56785678 in the intermediate computer and the address is changed to the address of the second computer. *Id.* at 12:6–8. “The new outer source address s-addr-2 (212.90.65.1) is substituted for the outer source address n-addr-1 (195.1.2.3), and the new outer destination address s-addr-3 (103-6-5-4) is substituted for the outer destination address c-addr-2 (212.90.65.1).” *Id.* at 12:13–17. Moreover, “[t]he new SPI value, s-SPI-3 (0x56785678), is substituted for the SPI value c-SPI-2 (0x12341234).” *Id.* at 12:17–18. The invention accomplishes the effect of “double tunneling,” while maintaining confidentiality of packets with no extra overhead compared to standard IPsec. *Id.* at 10:23–28.

C. Illustrative Claim

Petitioner challenges claims 1 and 2 of the '397 patent. Claim 1 is the sole independent claim and claim 2 depends from claim 1. Claim 1 is reproduced below.

1. A method for secure forwarding of a message in a secure connection via an intermediate computer, comprising:
 - a first computer and a second computer establishing a secure connection by negotiating and exchanging keys with one

another according to a key exchange protocol via the intermediate computer,

the intermediate computer receiving a secure message having a first source address sent to an address of the intermediate computer,

the intermediate computer reading an unique identity from the secure message,

the intermediate computer finding a destination address of the secure message by using the unique identity, and

the intermediate computer sending the secure message in the secure connection to the destination address by using the address of the intermediate computer as a second source address.

Ex. 1001, 22:41–58.

D. Asserted Ground of Unpatentability

Petitioner asserts that claims 1 and 2 are unpatentable based on the following ground. Pet. 6:

References	Basis ¹	Challenged Claims
RFC3104 ² and Grabelsky ³	§ 103(a)	1 and 2

II. DISCUSSION

A. Claim Construction

In this *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claims in a civil

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the ’397 patent has an effective filing date before the effective date of the applicable AIA amendments, we refer to the pre-AIA versions of 35 U.S.C. § 103.

² RFC3104, “RSIP Support for End-to-end IPsec,” Oct. 2001 (Ex. 1004, “RFC3104”).

³ U.S. Patent No. 7,032,242 B1, issued Apr. 18, 2006 (Ex. 1005, “Grabelsky”).

action under 35 U.S.C. § 282(b). *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51,340, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). The claim construction standard includes construing claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005).

For purposes of this Decision, we need not expressly construe any claim terms. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that “only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”); *see also Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs.* in the context of an *inter partes* review).

B. Principles of Law

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;

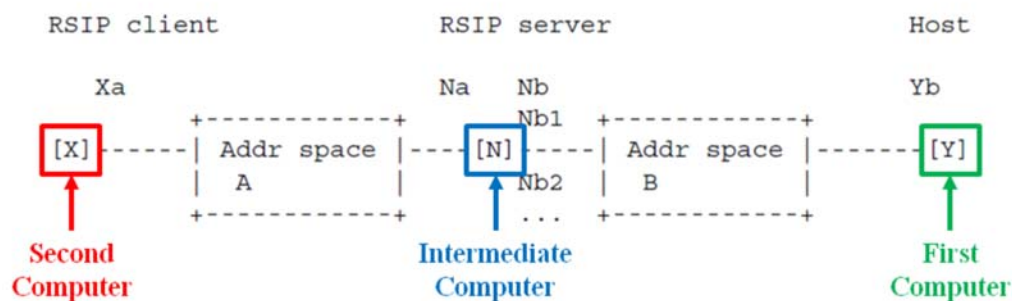
(3) the level of ordinary skill in the art;⁴ and (4) when in evidence, objective indicia of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. Asserted Obviousness of Claims 1 and 2 over RFC3104 and Grabelsky

Petitioner contends claims 1 and 2 are unpatentable under 35 U.S.C. § 103(a) as obvious over RFC3104 and Grabelsky. Pet. 17–41. In support of its showing, Petitioner relies upon the Declaration of Dr. Goldschlag. *Id.* (citing Ex. 1002).

1. RFC3104

RFC3104 is a technical document that “proposes mechanisms that enable Realm Specific IP (RSIP) to handle end-to-end IPsec (IP Security).” Ex. 1004, 1. Petitioner’s annotated RFC3104 diagram (Pet. 26) is reproduced below:



⁴ Relying on the testimony of Dr. David Goldschlag, Petitioner offers an assessment as to the level of skill in the art at the time of the '397 patent. Pet. 14 (citing Ex. 1002 ¶¶ 29–30). Patent Owner does not propose an alternative assessment. *See generally* Prelim. Resp. To the extent necessary, and for purposes of this Decision, we accept the assessment offered by Petitioner as it is consistent with the '397 patent and the asserted prior art.

Petitioner's annotated RFC3104 diagram shows Hosts X and Y that belong to different address spaces A and B. Ex. 1004, 3. N is an RSIP server that has two addresses: Na on address space A and Nb on address space B. *Id.* RFC3104 "proposes RSIP extensions and mechanisms to enable an RSIP client X to initiate IKE and IPsec sessions to a legacy IKE and IPsec node Y." *Id.* RFC3104 "assumes that RSIP server N is examining a packet sent by Y, destined for X." *Id.* RSIP client and server N arrive at an SPI value to denote the incoming IPsec security association from Y to X. *Id.* at 5. When "N and X make sure that the SPI is unique within both of their SPI spaces, X communicates its value to Y as part of the IPsec security association establishment process, namely, Quick Mode in IKE . . . or manual assignment." *Id.* Y sends IPsec packets to X via address Nb using the negotiated SPI. *Id.* IPsec packets from Y to X arrive at RSIP server N for demultiplexing. *Id.* Packets are demultiplexed based on a minimum tuple of demultiplexing fields: protocol (50 or 51), SPI, and destination IP address. *Id.* If N finds a matching map it tunnels the packet to X according to the tunneling mode in effect. *Id.*

2. Grabelsky

Grabelsky is directed to a method and system for distributed network address translation with security features that allows IPsec to be used with distributed network address translation. Ex. 1005, code (57). Grabelsky Figure 1 is reproduced below.

FIG. 1

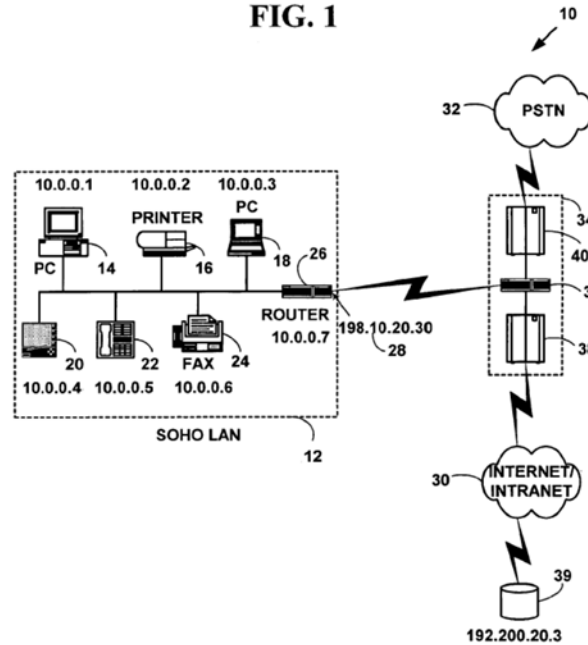


Figure 1 is an illustration of a network system for distributed address translation. *Id.* at 5:35–36. Network 10 includes first computer network 12 with multiple network devices (14, 16, 18, 20, 22, 24) and router 26 to route data packets to another external computer network. *Id.* at 6:30–35.

Grabelsky describes security measures that can be used in its packet routing techniques, including IPsec. *Id.* at 20:42–45. Grabelsky describes receiving packets using IPsec at router 26, which maintains a mapping between local IP addresses of network devices (e.g., 14, 16, 18, 20, 22, 24) and SPI values. *Id.* at 32:33–36. When an AH or ESP IPsec packet arrives at router 26, router 26 examines a SPI value in the IPsec packet’s outermost header and determines a local IP 54 address of a destination network device. *Id.* at 32:36–42.

3. Discussion

Claim 1 recites “the intermediate computer receiving a secure message having a first source address *sent to an address of the intermediate computer*” and “the intermediate computer sending the secure message in

the secure connection to the destination address *by using the address of the intermediate computer as a second source address.*” The parties agree, as do we, that the “address of the intermediate computer” recited in the first phrase is the same “address of the intermediate computer” recited in the second phrase. Pet. 39; Prelim. Resp. 7–8.

For the first phrase, Petitioner contends that “a message sent to RSIP server N is sent originally to Nb and then sent to Na, both of which are considered addresses of RSIP server N that the message was sent to.” Pet. 28–29 (citing Ex. 1002 ¶ 88). For the second phrase, Petitioner contends that “when a message sent from Y to X is received by RSIP server N on the Nb interface, it must also be sent to the Na interface so that the Na interface can ultimately send the message to Client X.” *Id.* at 39 (citing Ex. 1002 ¶ 105). Petitioner further contends that “a POSITA would have understood that a secure message sent to RSIP server N (i.e., *the intermediate computer*) via address Nb is also sent to address Na as part of RFC3104’s ‘tunneling’ operation.” *Id.* at 40 (citing Ex. 1002 ¶ 106).

Petitioner recognizes that RFC3104 describes when a secure message is sent from Y to the intermediate computer (RSIP server N), it is sent to address Nb of the intermediate computer. Pet. 28–29. Petitioner contends, however, that the same secure message also is sent to address Na by the intermediate computer, and, therefore, the address Na meets the claimed “address of the intermediate computer.” *Id.* at 40.

We agree with Patent Owner that RFC3104 does not describe any message ever being sent from address Nb to address Na, or that RSIP server N (the intermediate computer) sends or even can send any message from itself to itself. Prelim. Resp. 15. Petitioner does not identify any such description in RFC3104. Rather, Petitioner relies on Dr. Goldschlag’s

testimony in support of Petitioner’s assertion that a person having ordinary skill in the art would have understood that a secure message sent to RSIP server N via address Nb is also sent to address Na as part of RFC3104’s tunneling operation. Pet. 39–40 (citing Ex. 1002 ¶¶ 105–106).

Dr. Goldschlag’s testimony, however, is conclusory and unsupported by record evidence. Ex. 1002 ¶¶ 105–106. For example, Dr. Goldschlag does not explain how RFC3104’s “tunneling” operation results in the understanding that a message sent to RSIP server N via address Nb is also sent to address Na. *Id.*⁵ Dr. Goldschlag’s testimony provides no factual basis in support of the assertion that a person having ordinary skill in the art would have understood that tunneling as described in RFC3104 means that a message sent to server N via address Nb is also sent to address Na. Such *ipse dixit* is insufficient to show a reasonable likelihood of success. See *Securus Techs. Inc. v. Glob. Tel*Link Corp.*, 701 F. App’x 971, 974–76 (Fed. Cir. 2017) (affirming the Board’s determination that conclusory testimony by an expert witness was insufficient to satisfy Petitioner’s burden of showing that the skilled artisan would have modified the references as asserted); see also 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”).

Petitioner proffers no other evidence that “tunneling” or “tunneling” operations would have been understood to mean that a computer, such as an

⁵ In contrast, Dr. Goldschlag testifies that in tunneling mode, packets that may originate at other hosts are “encapsulated” by adding a second AH or ESP header to the front of the packet. Ex. 1002 ¶ 37. The ’397 patent also describes tunneling in the context of an original packet being encapsulated. Ex. 1001, 3:35–37.

intermediate computer as claimed, sends a message from itself to itself, e.g., from one interface/address to another interface/address, as Petitioner alleges. See Pet. 39–40 (citing Ex. 1002 ¶ 105). Thus, we agree with Patent Owner that Petitioner has not shown how the prior art meets the above claim phrases.

For all of these reasons, we are not persuaded that Petitioner has established a reasonable likelihood that Petitioner would prevail in its challenge to claims 1 and 2 as unpatentable under 35 U.S.C. § 103(a) based on RFC3104 and Grabelsky.⁶

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not shown a reasonable likelihood that it would prevail in showing that claims 1 and 2 of the '397 patent are unpatentable.

IV. ORDER

For the foregoing reasons, it is
ORDERED that the Petition is *denied* as to all challenged claims, and no trial is instituted.

⁶ Because we find Petitioner has not shown a reasonable likelihood of prevailing on the challenge for the reasons discussed above, we do not reach Patent Owner's remaining arguments for this challenge.

IPR2019-00825
Patent 9,762,397 B2

PETITIONER:

Michael D. Specht
Daniel S. Block
Steven M. Pappas
STERNE, KESSLER, GOLDSTEIN & FOX, P.L.L.C.
mspecht-ptab@sternekessler.com
dblock-ptab@sternekessler.com
spappas-ptab@sternekessler.com

PATENT OWNER:

James T. Carmichael
CARMICHAEL IP LAW, PLLC
jim@carmichaelip.com

Christopher J. Lee
Richard B. Megley
Brian E. Haan
Ashley E. LaValley
LEE SHEIKH MEGLEY & HAAN LLC
clee@leesheikh.com
rmegley@leesheikh.com
bhaan@leesheikh.com
alavalley@leesheikh.com

Kenneth J. Weatherwax
Patrick Maloney
Jason C. Linger
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com
linger@lowensteinweatherwax.com