

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE, INC.,

Petitioner,

v.

VIRNETX, INC.,

Patent Owner.

Case IPR2017-00337
Patent 9,038,163 B2

Before KARL D. EASTHOM, KEVIN W. CHERRY¹, and
KEVIN C. TROCK, *Administrative Patent Judges*.

TROCK, *Administrative Patent Judge*.

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

¹ Judge Cherry replaced Judge Bisk on the panel following the hearing.

I. INTRODUCTION

Apple, Inc., (“Petitioner”) filed a request for an *inter partes* review of claims 1–10, 12–18, 21–31, 33–39, and 42 (the “challenged claims”) of U.S. Patent No. 9,038,163 B2 (Ex. 1001, “the ’163 patent”). Paper 1 (“Pet.”). VirnetX, Inc. (“Patent Owner”) filed a Preliminary Response to the Petition. Paper 7 (“Prelim. Resp.”). We instituted an *inter partes* review of the challenged claims of the ’163 patent. Paper 8 (“Dec. Inst.”). Patent Owner filed a Patent Owner Response (Paper 17, “PO Resp.”) and Petitioner filed a Petitioner Reply (Paper 21, “Pet. Reply”). On February 27, 2018, a hearing was held, a transcript of which has been entered into the record. Paper 30 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6(b). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). Having reviewed the arguments of the parties and the supporting evidence, we find that Petitioner has demonstrated by a preponderance of the evidence that each of challenged claims, 1–10, 12–18, 21–31, 33–39, and 42, of the ’163 patent are unpatentable.

A. *The ’163 Patent*

The ’163 patent’s specification (the “Specification”) focuses on techniques for securely communicating over the Internet based on a protocol called the “Tunneled Agile Routing Protocol” or “TARP.” Ex. 1001, 3:20–23. According to the Specification, TARP allows for secure and anonymous communications by using tunneling, an IP address hopping scheme where the IP addresses of the end devices and routers participating in the system can change over time, and a variety of other security

techniques. Ex. 1001, 1:38–40, 3:20–6:14. Two sections of the Specification—primarily spanning columns 39 to 42 and 49 to 53—are directed to techniques for establishing secure communications in response to DNS requests specifying a secure destination. *See* Ex. 1001, 39:26–42:16, 49:27–53:35. These portions of the Specification discuss the idea of modifying a “conventional DNS server” to include additional functionality that allows it to support the creation of virtual private networks. *See* Ex. 1001, 40:21–54. According to the Specification, a “modified DNS server” (*id.*, 40:25–29) receives a request to look up a network address associated with a domain name (*id.*, 39:26–31, 40:4–20, 4:31–49), determines whether a secure site has been requested (for example, by checking an internal table of sites) (*id.*, 40:33–37, 51:37–41), and then performs additional steps to support establishing a “virtual private network” with the secure site. *See* Ex. 1001, 41:22–39, 51:60–66. The Specification also describes several optional features of this system, such as using “IP hopblocks” to create a VPN or incorporating user authentication. Ex. 1001, 40:21–30, 49:41–51, 52:53–57. The Specification also describes different ways of implementing this “modified DNS server,” including through a single standalone DNS server as well as a distributed system incorporating a “conventional DNS server function” and a DNS proxy server. *Id.* at 40:21–30.

B. Challenged Claims of the '163 Patent

Petitioner challenges claims 1–10, 12–18, 21–31, 33–39, and 42 of the '163 patent. Challenged claims 1 and 22 are independent. Although similar, Claim 1 is directed to a method and claim 22 is directed to a system. Claim 1 is illustrative and is reproduced below.

1. A method of connecting a first network device and a second network device over a communication network, the method comprising:

receiving, from the first network device over the communication network, a request to look up a network address of the second network device based on an identifier associated with the second network device;

evaluating the request to determine whether the identifier is registered with a name service, connected to the communication network, that facilitates resolving the identifier and that further facilitates establishing direct encrypted communication links;

determining, based on the evaluation, whether the second network device is available to communicate through a direct encrypted communication link facilitated by the name service; and

based on a determination that the second network device is available, facilitating the establishment of the direct encrypted communication link between the first network device and the second network device, the facilitating the establishment of the direct encrypted communication link including provisioning the first network device or the second network device with one or more resources for the direct encrypted communication link,

wherein the established direct encrypted communication link carries encrypted data communicated between the first network device and the second network device, and the first network device is a user device.

Ex. 1001, 56:9–28.

II. DISCUSSION

A. Claim Construction

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. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct.

2131, 2144–46 (2016) (upholding the use of the broadest reasonable construction as the standard to be applied for claim construction in *inter partes* reviews). “Under a broadest reasonable interpretation, words of the claim must be given their plain meaning, unless such meaning is inconsistent with the specification and prosecution history.” *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1062 (Fed. Cir. 2016). Only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy. *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

In our Decision on Institution, we did not find it necessary at that point in the proceeding to construe expressly any claim terms or to adopt any proposed constructions. See Dec. Inst. 6. Rather, we applied the terms’ plain and ordinary meanings, as understood by one of ordinary skill in the art in light of the specification. *Id.* Patent Owner did not respond to Petitioner’s constructions presented in the Petition. PO Resp. 2. For purposes of this Final Written Decision, we continue to apply the plain and ordinary meanings of the claim terms.

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991).

Petitioner argues a person of ordinary skill in the art in the field of the ’163 patent

would have been someone with a good working knowledge of networking protocols, including those employing security techniques, as well as computer systems that support these protocols and techniques. The person also would be very familiar with Internet standards related to communications and security, and with a variety of client-server systems and technologies. The person would have gained this knowledge either through education and training, several years of practical working experience, or through a combination of these.

Pet. 8 (citing Ex. 1003 ¶ 83).

In Patent Owner's Response, Patent Owner does not propose directly a particular level of ordinary skill in the art with respect to the '163 patent. *See generally* PO Resp. 1–34. Patent Owner, however, does cite to a declaration by Dr. Fabian Monroe concerning what a person of ordinary skill in the art would have understood with respect to the prior art. *See e.g.*, PO Resp. 3, 15, 17 (citing Ex. 2002 ¶¶ 36, 57, 52–61, respectively). Dr. Monroe's declaration, however, does not indicate that Dr. Monroe reviewed the '163 patent or the challenged claims. *See* Ex. 2002 ¶¶ 1–3.

Based on the evidence of record, including the prior art references, we find that a person of ordinary skill in the art in the field of the '163 patent is a person who has a good working knowledge of networking protocols, including those employing security techniques, as well as computer systems that support these protocols and techniques, and is very familiar with Internet standards related to communications and security, with a variety of client-server systems and technologies, having gained this knowledge either through education and training, several years of practical working experience, or through a combination of these.

C. Alleged Grounds of Unpatentability

Petitioner alleged a single ground of unpatentability, namely that

claims 1–10, 12–18, 21–31, 33–39, and 42 of the '163 patent are unpatentable as obvious under 35 U.S.C. § 103 over the combined teachings of U.S. Patent No. 6,496,867 (Ex. 1007, “Beser”), “Security Architecture for the Internet Protocol,” (Ex. 1008, “RFC 2401”), “SIP: Session Initiation Protocol” (Ex. 1013, “RFC 2543”), and knowledge held by a person of ordinary skill in the art. Pet. 2. In our Decision on Institution, we instituted *inter partes* review on all the challenged claims alleged unpatentable in the Petition based on this ground. Dec. Inst. 20.

D. Prior Art References

1. Beser (Ex. 1007)

Beser describes a tunneling system that establishes an IP (internet protocol) tunneling association over a public network such as the Internet between two end devices 24 and 26 on private networks. Ex. 1007, 3:60–4:19, Abstract, Fig. 1. Beser’s system provides security for “[c]ompanies who cannot afford a private network [and] often transfer sensitive corporate information over the Internet.” *Id.* at 1:18–20.

Figure 1 of Beser follows:

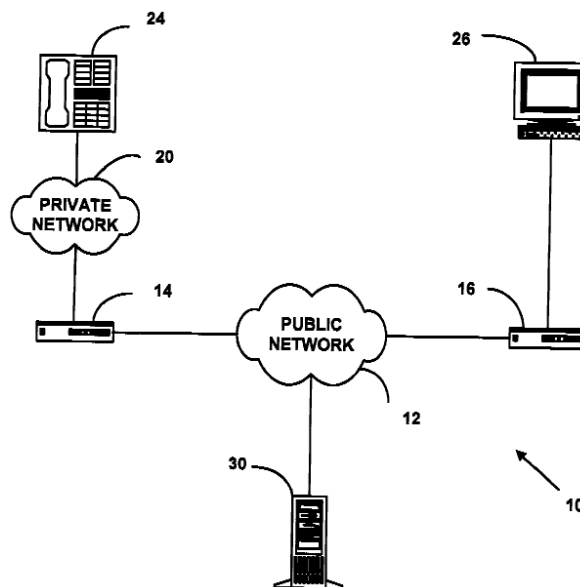


Figure 1 of Beser's system depicts public network 12 (for example the Internet), network end devices 24 and 26 on private network 20, trusted-third-party device 30, and modified edge routers or gateway network devices 14 and 16. *See* Ex. 1007, Abstract, 3:60–4:18. Edge routers 14 and 16 route packets between Internet or public network 12 and private network 20 that include terminating end devices such as 24 and 26. *See id.* at 4:18–23.

Beser's system "increases the security of communication on the data network" by providing and hiding, in packets, "private addresses" for originating device 24 and terminating device 26 on the network. *Id.* at Abstract, Fig. 1, Fig. 6. To begin a process for a secure transaction, at step 102, requesting device 24 may send to network device 14, as part of its request on a protocol layer below an application layer, an indicator that may be a "distinctive sequence of bits [that] indicates to the tunneling application that it should examine the request for its content and not ignore the datagram." Ex. 1007, 8:40–44, Figs. 1, 4. The request (which may include a series of packets) also includes a unique identifier, such as a domain name, employee number, telephone number, or social security number, and a public IP address 58 or other similar identifier associated with terminating device 26. Ex. 1007, 10:37–11:8, 11:9–12. At step 104, network device 14 informs trusted-third-party network device 30 of the request. *See id.* at 7:64–8:7, 11:9–20, Fig. 4.

Trusted-third-party device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network devices 16 and terminating devices 26. *See id.* at 11:32–58. At step 106 (and parallel step 116), DNS 30 associates terminating network device 26, based on its unique identifier (e.g., domain name, or other

identifier) in the request, with a public IP address for router device 16 (i.e., the association of the domain name with other stored information, including Internet addresses, shows they are connected together at the edge of public network 12). *See* Ex. 1007, 11:26–36, Figs. 1, 4, 5.² As indicated, DNS 30 includes, in a directory database or otherwise, stored public IP addresses for router 16 and terminal device 26 and other data that associates devices 16 and 26 together. *Id.* at 11:48–52. In other words, trusted-third-party network device DNS 30, includes the “IP 58 addresses for the terminating . . . device[s] 26,” and uses “data structures . . . known to those skilled in the art . . . for the association of the unique identifiers [for terminating devices 26] and IP 58 addresses for the . . . network devices 16”—including domain names as unique identifiers, as noted above. *Id.* at 11:2–5, 32–36, 48–55.

At step 108 (or step 118), Beser’s system assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *See id.* at 11:59–12:19, 12:38–48, Figs. 4, 5. In an exemplary embodiment, trusted-third-party network (DNS) device 30 performs the negotiation for private addresses in order to further ensure anonymity of end devices 24 and 26 (though device 30 need not be involved in the negotiation in one embodiment). *Id.* at 9:29–35, 12:17–19. The negotiated private IP addresses are “isolated from a public network such as the Internet,” and “are not globally routable.” *Id.* at 11:63–65. “These IP 58 addresses may be stored in network address tables on the respective network devices, and may be associated with physical or local network addresses for the respective

² Figure 5, which includes step 116, involves a specific Voice-over-Internet-Protocol (VoIP) application of the general process of Figure 4, which includes parallel step 106. *See* Ex. 1007, 3:26–30.

ends of the VoIP [(Voice-over- Internet-Protocol)] association by methods known to those skilled in the art.” *Id.* at 12:33–37.

The negotiated private IP addresses may be “inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network 12.” *Id.* at 12:15–16. The IP packets “may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12.” *Id.* at 11:22–25; *see also* 20:11–14 (disclosing encryption or authentication of first IP 58 packet to ensure hiding the address of the public IP address of network device 16). Beser also discloses, as background prior art, known forms of encryption for “the information inside the IP packets,” including IP Security (“IPSec”). *Id.* at 1:54–56.

Beser describes edge routers, such as network devices 14 and 16, as devices that route packets between public networks 12 and private networks 20. *Id.* at 4:18–24. End devices 24 and 26 include network multimedia devices, VoIP devices, or personal computers. *Id.* at 4:43–54.

2. RFC 2401 (*Exhibit 1008*)

RFC 2401 is a request for comments concerning security architecture for the Internet protocol. RFC 2401 “specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer.” Ex. 1008, 3. According to RFC 2401, IPsec provides a “set of security services,” including “access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption).” Ex. 1008, 4. RFC 2401 describes IPsec further, as follows:

IPsec allows the user (or system administrator) to control the granularity at which a security service is offered. For example, one can create a single encrypted tunnel to carry all the traffic between two security gateways or a separate encrypted tunnel can be created for each TCP connection between each pair

of hosts communicating across these gateways.

Id. at 7.

The “security services use shared secret values (cryptographic keys) . . . (The keys are used for authentication/integrity and encryption services).” *Id.*

3. RFC 2543 (*Exhibit 1013*)

RFC 2543 is a request for comments concerning the Session Initiation Protocol (SIP). RFC 2543 “specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvement.” Ex. 1013, 1. RFC 2543 explains that the SIP “is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these.” *Id.*

RFC 2543 explains that SIP supports five facets of establishing and terminating multimedia communications:

User location: determination of the end system to be used for communication;

User capabilities: determination of the media and media parameters to be used;

User availability: determination of the willingness of the called party to engage in communications;

Call setup: "ringing", establishment of call parameters at both called and calling party; [and]

Call handling: including transfer and termination of calls.

Ex. 1013, 7–8.

D. Obviousness of the Challenged Claims

1. Independent Claims 1 and 22

Petitioner contends that independent claims 1 and 22 of the '163 patent would have been obvious over the combination of Beser, RFC 2401, and RFC 2543. Pet. 41–55. Claims 1 and 22 are markedly similar. Claim 1 recites a method of connecting two network devices over a communication network through a direct encrypted communication link. Ex. 1001, 56:9–28. Claim 22 recites a system configured to execute similar steps, but also recites some system limitations not found in claim 1. Ex. 1001, 57:43–58:6. We consider the limitations claims 1 and 22 have in common below, as well as the system limitations found in claim 22.

a. Preamble of Claim 1

With respect to the preamble of claim 1, Petitioner relies on Beser to teach “connecting a first network device and a second network device over a communication network.” Pet. 41–42; Ex. 1007, 8:15–20, 21:52–62, 22:2–22; Ex. 1003 ¶¶ 129, 133–134. The process described in Beser begins when a user sends a request through the originating end device by, for example, initiating a VoIP call. Ex. 1007, 10:2–4, 10:22–36, 10:57–66; Ex. 1003 ¶ 133. The request is processed by a third-party network device, which, with the help of the first and second network devices, establishes a private tunneling association between the end devices, enabling the originating end device to connect to and communicate with the terminating end device. Ex. 1007, 8:15–20, 14:51–67, 19:21–37, 23:15–25; Ex. 1003 ¶¶ 133–134.

Patent Owner does not contest specifically Petitioner’s evidence with respect to the preamble. See PO Resp. 2–6. Rather, Patent Owner acknowledges that Beser involves initiating a tunneling association between

an originating end and a terminating end facilitated by an intermediary, trusted-third-party network device. PO Resp. 3.

Based on this evidence, Petitioner has shown sufficiently that Beser's user sending a request to initiate a VoIP call from an originating device through a network to connect with an end device teaches or suggest the preamble's "connecting a first network device and a second network device over a communication network."

b. *"receiving, from the first network device..., a request to look up a network address of the second network device based on an identifier associated with the second network device"*

With respect to the limitation "receiving, from the first network device..., a request to look up a network address of the second network device based on an identifier associated with the second network device," Petitioner relies on Beser originating end device ("first network device") sending a request to initiate a VoIP tunneling association with a terminating end device ("second network device"). Pet. 42–43; Ex. 1007, 7:64–8:1, 9:64–10:41; Ex. 1003 ¶¶ 168, 172. This request, Petitioner explains, contains a unique identifier associated with the terminating end device ("an identifier associated with the second network device"). *Id.*; Ex. 1007, 8:1–3, 10:37–11:8; Ex. 1003 ¶¶ 173–174. Petitioner further explains that Beser's unique identifier can be a domain name or a VoIP phone number (Ex. 1007, 10:37–42, 10:55–11:5), and the trusted third-party network device that processes the request can be a domain name server (*id.*, 4:9–11, 11:33–36). Pet. 43. Petitioner notes that the Specification describes the use of a "domain name" as an identifier in a DNS (Domain Name Server) request. *Id.*; see Ex. 1001, 39:34–40, 40:34–40; Ex. 1003 ¶¶ 131–132.

Patent Owner argues that Beser's request is to initiate a tunneling connection, and "is not 'a request to look up an internet protocol (IP) address' of the terminating end device based on a domain name associated with the terminating end device." PO Resp. 6–7 (citing Ex. 2002 ¶ 41). Patent Owner argues that "*Beser* only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, it associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26," because "there is no 'look up' of the private IP address for terminating device 26." *Id.* at 8–9 (citing Ex. 1007, 11:26–32, 12:2–4; Ex. 2002 ¶¶ 43–44). The private IP address for terminating device 26, Patent Owner argues, is simply *assigned* to the terminating device. *Id.* at 8.

Beser, however, states expressly that "the trusted-third-party network device 30 is . . . a domain name server." Ex. 1007, 11:33–34. As Dr. Tamassia testifies, typical domain name server functionality includes looking up IP addresses to assign them a unique identifier. *See* Ex. 1003 ¶¶ 95–101. In *Beser*, the tunneling request sent by originating device 24 is a "request to look up a network address" because in response to receiving the request, the *Beser* trusted device 30 looks up at least two IP addresses.³ First, it consults an internal database of registered devices to look up the IP address of second network device 16 that is associated with the unique identifier. Ex. 1007, 11:45–58. Second, it looks up a private IP address for terminating device 26 by sending a message to network device 16 requesting

³ *Beser* also discloses other unique identifiers for a look up related to terminating device 26, including, *inter alia*, a "domain name" and a "previously assigned public IP 58 address." Ex. 1007, 10:41–11:2.

the address. Ex. 1007, 9:29–30, 12:16–19, 14:14–27, Figs. 6 and 9. As a result of this process, originating device 24 receives an IP address for terminating device 26. Ex. 1007, 21:48–52.

Patent Owner’s argument that the private address for terminating device 26 is simply “assigned” without involving a “look up” is not persuasive because the trusted device 30 “looks up” the IP address when it sends a message to network device 16 requesting a private IP address. Ex. 1007, Fig. 9 (packets 164 & 166), 13:33–48, 13:66–14:18. Moreover, second device 16 does not simply “assign” an IP address—it looks one up by selecting an unused address out of a pool of IP addresses. Ex. 1007, 13:49–64.

Based on this evidence, Petitioner has shown sufficiently that Beser’s user sending a request to initiate a tunneling association from an originating device through a network to connect with an end device teaches or suggests the recited limitation “receiving, from the first network device..., a request to look up a network address of the second network device based on an identifier associated with the second network device,”

- c. *“evaluating the request to determine whether the identifier is registered with a name service,” that “facilitates resolving the identifier and that further facilitates establishing direct encrypted communication links”*

With respect to the limitation “evaluating the request to determine whether the identifier is registered with a name service,” that “facilitates resolving the identifier and that further facilitates establishing direct encrypted communication links,” Petitioner relies on Beser’s explanation that a trusted-third-party network device can be a domain name server that functions according to industry standards (Pet. 45; Ex. 1007, 4:55–63,

11:32–36; Ex. 1003 ¶¶ 158–161), but is modified to maintain a database of subscribers, (Ex. 1007, 11:48–52). Beser’s database, Petitioner explains, correlates each subscriber’s registered unique identifier to “the IP 58 address of a particular second network device 16” and may also include “public IP 58 addresses for the terminating telephony device 26.” Pet. 45; Ex. 1007, 11:48–52; 8:65–9:1, 11:26–44; Ex. 1003 ¶¶ 162–165.

Petitioner argues that Beser teaches, in response to each tunneling request, the trusted-third-party network device parses the request to evaluate and determine whether the unique identifier is listed in its internal database of registered users or devices (“evaluating. . . whether the identifier is registered”). Pet. 45; Ex. 1007, 11:30–36, 11:45–58; Ex. 1003 ¶ 165. Petitioner notes the Specification describes a similar evaluation by checking a domain name against an internal table of secure sites. Pet. 45; *see* Ex. 1001, 40:33–37. Petitioner explains that if the unique identifier is registered as a subscriber, the trusted-third-party device 30 will negotiate with the first and second network devices to establish an IP tunnel between those network devices. Pet. 45; Ex. 1007, 9:6–11, 11:59–62; 9:26–30, 11:9–44; Ex. 1003 ¶¶ 165–166, 178–180.

Patent Owner argues that before assigning the public IP address of device 16 to the unique identifier, Beser never checks whether the identifier is registered with the third party device 30. PO Resp. 11 (citing Ex. 1007, 11:26–32, 11:45–57). Moreover, Patent Owner argues, Beser never suggests that this data structure is looked up when the tunnel request is received by device 30. *Id.* (citing Ex. 2002 ¶ 44; Ex. 1007, 11:45–57).

Beser’s trusted third-party network device, however, includes a modified domain name server that maintains a database of subscribers.

Ex. 1007, 4:55–63, 11:32–36, 11:48–52; Ex. 1003 ¶¶ 158–161. The database maps each subscriber’s unique identifier to IP addresses including associated IP addresses for the second network device and terminating device. Ex. 1007, 11:48–52; Ex. 1003 ¶¶ 162–165. Upon receipt of a tunneling request, the trusted-third-party network device searches the database for the entry that matches a registered unique identifier. Ex. 1007, 11:45–58. If the unique identifier is registered—matches an entry—as a subscriber of the modified domain name server, the trusted-third-party network device negotiates to establish a tunnel between those network devices using the IP addresses. Ex. 1007, 9:6–11, 11:59–62, 9:26–30, 11:9–36; Ex. 1003 ¶¶ 165–166, 178–180.

Based on this evidence, Petitioner has shown sufficiently that Beser teaches or suggests the recited limitation “evaluating the request to determine whether the identifier is registered with a name service,” that “facilitates resolving the identifier and that further facilitates establishing direct encrypted communication links.”

d. “determining . . . whether the second network device is available to communicate through a direct encrypted communication link facilitated by the name service”

With respect to the limitation “determining, based on the evaluation, whether the second network device is available to communicate through a direct encrypted communication link facilitated by the name service,” Petitioner relies on Beser combined with RFC 2401 and RFC 2543’s protocol for establishing a VoIP connection. Pet. 46. Petitioner asserts that Beser suggests this configuration by describing an embodiment where a tunneling request is a VoIP request having a system compatible with IETF

(Internet Engineering Task Force) standards. Pet. 46; Ex. 1007, 4:55–62, 10:2–4. In this configuration, Petitioner explains, the originating and terminating devices are SIP user agents, and the first and second network devices are SIP proxy servers. *Id.*; Ex. 1003 ¶ 256. Petitioner asserts that when the Beser originating device initiates an IP tunnel for a VoIP call, it generates an INVITE message per RFC 2543, which then serves as a VOIP request to initiate the VoIP association. Pet. 46; Ex. 1007, 10:2–6.

In this configuration, Petitioner explains, after the trusted-third-party network device determined the unique identifier was registered, it would look up the public IP address of the second network device. Pet. 47; Ex. 1003 ¶¶ 258–260. The VoIP request (in Beser, the INVITE message) would then be sent to the second network device. *Id.* Petitioner asserts that this message could be sent by the trusted-third-party network device, as shown in Beser Figure 9, or it could be sent by the first network device, as shown in Figure 14. *Id.* Petitioner asserts that before selecting a private IP address for the terminating device, the second network device would process the INVITE message according RFC 2543. Pet. 47; Ex. 1003 ¶ 261. The second network device would then forward the message to the terminating end device, causing it to ring. *Id.*; Ex. 1013, 16, 75. If the user answered the phone, Petitioner asserts, it would return a success status message to the second network device as taught by RFC 2543. Pet. 47; Ex. 1013, 76, 92–94.

Petitioner argues that in the combined system of Beser, RFC 2401, and RFC 2543, a device that is registered with device 30 supports “encrypted communication links” (i.e., it supports Beser’s IP tunnel configured to provide end-to-end encryption), and thus, if the user answers

the phone, that device is available for such a link. Pet. 48; see Ex. 1003 ¶¶ 237–241.

In its Response, Patent Owner does not respond specifically to Petitioner’s evidence with respect to this limitation. See generally PO Resp. 2–18.

Based on this evidence, Petitioner has shown sufficiently that Beser’s tunneling request to initiate a VoIP association sent to a second network device by a trusted-third-party network device, where the second network device forwards the message to the terminating end device, and if answered, return a success status message to the second network device, teaches or suggests the recited limitation “determining, based on the evaluation, whether the second network device is available to communicate through a direct encrypted communication link facilitated by the name service.”

- e. *“facilitating the establishment of the direct encrypted communication link between the first network device and the second network device”*

With respect to the limitation “based on a determination that the second network device is available, facilitating the establishment of the direct encrypted communication link between the first network device and the second network device, the facilitating . . . including provisioning the first network device or the second network device with one or more resources for the direct encrypted communication link, wherein the . . . link carries encrypted data communicated between the first network device and the second network device, and the first network device is a user device,” Petitioner relies on Beser and RFC 2401 to teach methods and systems that facilitate establishing a “direct encrypted communication link.” Pet. 50. Petitioner argues that it would have been obvious to configure the Beser IP

tunneling scheme to include end-to-end encryption of all IP traffic based on the teachings of RFC 2401, in order to ensure data security, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. Pet. 33–38, 50; Ex. 1003 ¶ 237; see Ex. 1008, 25.

Petitioner also asserts that in the combined system suggested by Beser, RFC 2401, and RFC 2543, a secure IP tunnel is established only if the unique identifier is registered with the trusted-third-party network device and the user at the terminating device answers the call. Pet. 52; Ex. 1007, 9:6–11, 9:26–30, 11:26–58; Ex. 1003 ¶¶ 177–180, 185.

Petitioner explains that during the negotiation of a tunnel IP in Beser, packets are exchanged among the trusted-third-party network device, the first network device, and the second network device. Pet. 52; Ex. 1007, 9:29–30, 12:55–58, 12:38–40, 13:6–13, 13:66–14:2; see also Figs. 9, 14; Ex. 1003 ¶¶ 195–197. Petitioner explains that the first network device will receive the private IP address for the terminating device only if that device is both registered and available. Pet. 52. Following the successful negotiation of the IP tunnel, “[b]oth first 14 and second 16 network devices have obtained the private IP 58 addresses of the originating end of the tunneling association 24 that requested the initiation of the tunneling association and the terminating end of the tunneling association 26 that was associated with the unique identifier.” Ex. 1007, 14: 57–62. The originating end device also receives both private IP addresses. *Id.* at 21:48–62.

Petitioner argues that the private IP addresses in Beser are the recited “one or more resources for the direct encrypted communication link” because they allow the originating and terminating end devices to

communicate through a private IP tunnel where communications are encrypted according to IPsec (i.e., information that enables communication in a virtual private network, where the virtual private network uses encryption). Pet. 53; Ex. 1003 ¶¶ 197, 237.

Petitioner argues that the combination of Beser, RFC 2401, and RFC 2543 shows that the communication link between the end devices carries “*encrypted data*,” because a person of ordinary skill in the art would have considered it obvious to include end-to-end encryption of all IP traffic in the Beser IP tunnel based on RFC 2401. Pet. 54; Ex. 1003 ¶¶ 231, 237. In this configuration, Petitioner asserts, data sent between the originating end device and the terminating end device would be encrypted. *Id. see* Ex. 1007, 21:15–25; Ex. 1008, 25; Ex. 1003 ¶¶ 237, 241.

Petitioner relies on Beser to show that the first network device is a “user device.” Pet. 54. Beser explains that the originating and terminating end devices can be telephony devices (including VoIP devices or personal computers running facsimile or audio applications) or multimedia devices (such as Web-TV sets and decoders, interactive video game players and personal computers running multimedia applications). Ex. 1007, 4:43–52; Ex. 1003 ¶ 138, 141–44, 167–68. Petitioner asserts that these are all devices that can be used directly by a user to establish and access an encrypted IP tunnel according to the combined teachings of Beser and RFC 2401. Ex. 1007, 8:15–20, 10:57–66 (describing a “user” using an end device).

With respect to this limitation, Patent Owner contests Petitioner’s combination of Beser, RFC 2401, and RFC 2543, arguing that it would not have been obvious to combine the cited art in the manner proposed by Petitioner. PO Resp. 12–18. Patent Owner argues that Beser teaches away

from using encryption to secure communications. *Id.* We consider Patent Owner's arguments with respect to Petitioner's proposed combination below.

f. Combination of Beser, RFC 2401, and RFC 2543

Petitioner asserts that a person of ordinary skill in the art would have found it obvious to combine Beser and RFC 2401 to provide end-to-end encryption in an IP tunnel between Beser's originating and terminating end devices. Pet. 33; Ex. 1003 ¶¶ 223, 227, 233–234. Petitioner argues that Beser makes clear that data sent via an IP tunnel is and ordinarily should be encrypted to protect the contents of communications. Pet. 33; Ex. 1007, 1:54–56, 2:6–14, 2:22–24; *see also id.*, 11:22–25, 18:2–5, 20:11–14. Beser's reference to IPsec as the standard protocol to encrypt communications, Petitioner argues, conveys that IPsec should be used with Beser's IP tunnel. Pet. 33; Ex. 1007, 1:54–58, 2:1–5, 2:36–45; Ex. 1003 ¶¶ 221–224.

Petitioner also asserts that a person of ordinary skill in the art would have found it obvious to combine RFC 2543 with Beser and RFC 2401 to allow for the efficient establishment of VoIP calls. Pet. 38; Ex. 1003 ¶¶ 252–264. Petitioner notes that in one of Beser's embodiments, the Beser architecture is used to setup a VoIP call between the originating and terminating devices pursuant to the H.323 VoIP standard. Pet. 38; Ex. 1007, 9:63–10:2. Petitioner points out that although Beser uses H.323 as an example, Beser states that its system can support other standards-based protocols such as those promulgated by the IETF (Internet Engineering Task Force). Pet. 39; Ex. 1007, 4:60–61, 4:67–5:1. The IETF has a VoIP protocol suite, and Petitioner asserts that RFC 2543 is one of the standards in

that suite. Pet. 39; Ex. 1003 ¶ 243. The skilled person, Petitioner argues, would have found it obvious to configure Beser to work with RFC 2543's call setup procedures, as this would have been simply substituting one well-known VoIP protocol (RFC 2543) for another (H.323) with predictable results. Pet. 39; Ex. 1003 ¶¶ 252–253.

Patent Owner argues that Petitioner's proposed combination is flawed because "*Beser* dismisses the idea of encryption entirely, noting that the 'expense of added computer power might also dampen the customer's desire to invest in VoIP equipment' at all." PO Resp. 14 (quoting Ex. 1007, 1:65–67; Ex. 2002 ¶ 55). Patent Owner also notes that *Beser* criticizes network address translation as a form of security because it is similarly "computationally expensive." *Id.* (quoting Ex. 1007, 2:22–23).

To solve these problems, Patent Owner argues, *Beser* proposed a method of hiding the addresses of originating and terminating devices. *Id.* (citing Ex. 2002 ¶ 57). By hiding the identities of the network devices, Patent Owner argues, "*Beser* touts that its method is able to increase communication security without increasing computational burden." *Id.* at 15 (citing Ex. 1007, 2:43–3:14). Thus, Patent Owner argues, one of ordinary skill in the art would have understood that *Beser* is directed to providing a method for securing communications other than encryption and teaches away from encryption. *Id.*

Patent Owner argues that *Beser*'s statement that "IP tunnels are and should ordinarily be encrypted" does not support Petitioner's position because this is limited to encryption being used to hide the identity of network devices, and is not directed to encryption of traffic in one of *Beser*'s tunnels. *Id.* at 16 (quoting Ex. 1007, 18:2–5). *Beser*, Patent Owner argues,

“does not use encryption in transmitting data over the established tunnel and, in fact, teaches away from using encryption in transmitting data.” *Id.* at 16–17.

Contrary to Patent Owner’s arguments, Beser recognizes that encryption ordinarily should be used when the contents of a communication need to be protected. *See* Ex. 1007, 1:54–56. Beser also teaches using encryption when user-identifiable data are sent over a network, such as during establishment of an IP tunnel. *Id.* at 11:22–25. Beser also criticizes prior art IP tunneling methods that sometimes prevent use of encryption, (*id.* at 2:1–8, 2:22–24), and states that its tunneling method is intended to overcome such problems (*id.* at 2:43–45).

Although Beser expresses concern that some prior art encryption and IP tunneling techniques may be computationally expensive, Beser’s design provides an improved method for ensuring user privacy by allowing communications over the Internet to be anonymous. *See* Ex. 1007, 2:36–40, 3:4–9. Beser explains that while encrypting data can protect the contents of communications, prior art encryption did not always provide privacy because it did not hide the identities of the devices that were communicating. *Id.* at 2:1–5, 1:56–58. Beser’s IP tunneling technique was designed to overcome these problems with the prior art. *Id.* at 2:43–45.

Beser notes that its IP tunnel can improve the security of encryption by helping to “prevent a hacker from intercepting all media flow between the ends” (*id.* at 2:36–40), and from “accumulating . . . sufficient information to decrypt the message” (*id.* at 1:56–58). Beser’s tunneling method is not technically incompatible with encryption, and a skilled person would be able to adjust a system’s configuration to accommodate the use of

encryption with Beser's IP tunnels. *See* Ex. 1003 ¶¶ 227–228; Ex. 1077, 79:3–11, 80:20–81:8, 82:7–17. Because Beser's IP tunnel has a low computational burden, a person of ordinary skill in the art would have understood that Beser's method is flexible and could be integrated into existing communications systems and combined with other security techniques. *See* Ex. 1003 ¶ 138; Ex. 1007, 3:4–9, 4:55–5:2.

A person of ordinary skill in the art reading Beser would have understood that using encryption would help protect the contents of communications in an IP tunnel. *See* Ex. 1003 ¶¶ 233–241. Based upon the evidence presented, Petitioner has shown sufficiently that configuring Beser's IP tunneling scheme to include end-to-end encryption of all IP traffic as provided by IPsec in RFC 2401, and incorporating SIP of RFC 2543, teaches or suggests the recited limitation “facilitating the establishment of the direct encrypted communication link between the first network device and the second network device, the facilitating . . . including provisioning the first network device or the second network device with one or more resources for the direct encrypted communication link, wherein the . . . link carries encrypted data communicated between the first network device and the second network device, and the first network device is a user device.”

g. Additional Limitations of Claim 22

Claim 22 recites specific computer system components, including “a memory,” “a network interface,” and “one or more processors configured to” carry out the recited steps of the claim. Ex. 1001, 57:43–48. Petitioner relies on Beser, asserting that Beser's systems are implemented using programmed computers and other programmable devices. Pet. 55; Ex. 1007,

4:7–5:2, 5:15–47. These network devices include at least one high speed Central Processing Unit (CPU) and a memory. Ex. 1007, 5:15–47. The network devices also include a network interface. *Id.*, 7:26–42, 12:32–36, 22:22–31; Ex. 1003 ¶¶ 136–137, 147–148.

In its Response, Patent Owner does not respond specifically to Petitioner’s evidence with respect to these additional system limitations of claim 22. *See generally* PO Resp. 2–18. Based on this evidence, Petitioner has shown sufficiently that Beser’s description of a CPU, memory, and a network interface teaches or suggests the additional recited system limitations of claim 22.

h. Conclusion on Independent Claims 1 and 22

For all the reasons stated above, we are persuaded that Petitioner has shown by a preponderance of the evidence that the combination of Beser, RFC 2401, and RFC 2543 teaches or suggests all the limitations of independent claims 1 and 22.

2. Dependent Claims

Petitioner contends that dependent claims 2–10, 12–18, 21, 23–31, 33–39, and 42 of the ’163 patent are obvious over the combination of Beser, RFC 2401, and RFC 2543. Pet. 55–64. Patent Owner contests Petitioner’s evidence with respect to several of the dependent claims. *See* PO Resp. 19–21.

a. Dependent Claims 2 and 23

Claims 2 and 23 depend from claims 1 and 22, respectively, and further specify that “the encrypted data includes at least one of video data, audio data, message data, or chat data.” Petitioner asserts that Beser teaches a variety of types of data can be transmitted through its IP tunnel including

VoIP traffic, “multimedia” content (e.g., video, audio), video conference traffic, or content for web pages (e.g., delivered to WebTV devices or decoders or personal computers). Pet. 55–56 (citing Ex. 1007, 4:43–54, 6:24–57, 9:64–10:2; Ex. 1003 ¶ 167). Petitioner argues that in the combined system suggested by Beser, RFC 2401, and RFC 2543, encrypted VoIP or video conference data are sent between the end devices. *Id.* at 56 (citing Ex. 1007, 4:55–61, 9:64–10:5; Ex. 1003 ¶¶ 237, 252–253).

Patent Owner argues that “*Beser* teaches away from using encryption and therefore must teach away from transmitted encrypted data on its tunnels.” PO Resp. 19 (citing PO Resp. Sec. III.D; Ex. 1007, 1:62–63; Ex. 2002 ¶ 62.)

We disagree with Patent Owner. As discussed above with respect to claim 1, *Beser* recognizes that encryption ordinarily should be used when the contents of a communication need to be protected. *See* Ex. 1007, 1:54–56. *Beser* also teaches using encryption when user-identifiable data are sent over a network, such as during establishment of an IP tunnel. *Id.* at 11:22–25. A person of ordinary skill in the art reading *Beser* would have understood that using encryption would help protect the contents of communications in an IP tunnel. *See* Ex. 1003 ¶¶ 233–241.

We are persuaded that Petitioner has shown by a preponderance of the evidence that *Beser*’s explanation that a variety of types of data can be transmitted through its IP tunnel, including VoIP traffic, multimedia content, video conference traffic, or content for web pages teaches or suggests the recited limitation “encrypted data includes at least one of video data, audio data, message data, or chat data,” of dependent claims 2 and 23.

b. Dependent Claims 3, 4, 24, and 25

Claims 3 and 24 depend from claims 1 and 22, respectively, and further specify that the “direct encrypted communication link is a communication link... in a virtual private network.” Claims 4 and 25 depend from claims 3 and 24, respectively, and further specify that “the virtual private network is an IPsec virtual private network.”

Petitioner asserts Beser shows that a trusted-third-party device, along with first and second network devices, is used to establish secure IP tunnels. Pet. 56 (citing Ex. 1007, 7:62–8:20). Petitioner asserts Beser’s trusted-third-party network device is connected to a public communication network. *Id.* (citing Ex. 1007, 8:3–12, Fig. 1). Petitioner asserts Beser’s IP tunnels allow end devices to communicate directly over a secure and anonymous channel. *Id.* (citing Ex. 1007, 8:15–20, 12:13–16, 22:2–8; Ex. 1003 ¶¶ 197–199). Petitioner argues a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401 (i.e., IPsec), in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *Id.* at 57.

Petitioner argues the combination of Beser, RFC 2401, and RFC 2543 shows a communication link that is part of a “*virtual private network*” (i.e., a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping). *Id.* (citing Ex. 1003 ¶¶ 237, 252–253). Petitioner argues RFC 2401 defines the IPsec standard, and therefore the combination also shows an “IPsec virtual private network.”

Id.

Patent Owner argues that “Beser teaches away from using encryption,” and therefore Petitioner has failed to establish that claims 3, 4, 24, and 25 are unpatentable. PO Resp. 20.

We disagree with Patent Owner that Beser teaches away from using encryption. As discussed above with respect to claim 1, Beser recognizes that encryption ordinarily should be used when the contents of a communication need to be protected. *See* Ex. 1007, 1:54–56. Beser also teaches using encryption when user-identifiable data are sent over a network, such as during establishment of an IP tunnel. *Id.* at 11:22–25. A person of ordinary skill in the art reading Beser would have understood that using encryption would help protect the contents of communications in an IP tunnel. *See* Ex. 1003 ¶¶ 233–241.

We are persuaded that Petitioner has shown by a preponderance of the evidence that the combination of Beser, RFC 2401, and RFC 2543 teaches or suggests the limitations “direct encrypted communication link is a communication link... in a virtual private network,” recited by dependent claims 3 and 24, and “the virtual private network is an IPsec virtual private network,” recited by claims 4 and 25.

c. Dependent Claims 5 and 26

Claims 5 and 26 depend from claims 1 and 22, respectively, and further specify that the secure communications service includes a “telephony service.” Petitioner asserts Beser explains that the originating and terminating end devices can be “telephony devices” including “VoIP devices (portable or stationary) or personal computers running facsimile or audio applications.” Pet. 57 (citing Ex. 1007, 4:43–52, Figs. 1 and 17).

With respect to claims 5 and 26, Patent Owner contends generally that “*Beser* and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded that Petitioner has shown by a preponderance of the evidence that *Beser*’s explanation that its originating and terminating end devices can be “telephony devices” including “VoIP devices (portable or stationary) or personal computers running facsimile or audio applications,” teaches the recited limitation “wherein the established direct encrypted communication link provides a telephony service,” of dependent claims 5 and 26. Pet. 57.

d. Dependent Claims 6, 7, 27, and 28

Claims 6 and 27 depend from claims 5 and 26, respectively, and further specify that the telephony service uses “modulation.” Claims 7 and 28 depend from claims 6 and 27, respectively, and further specify that “*the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).*”

Petitioner asserts *Beser* explains that VoIP or video conference data can be transmitted through an IP tunnel, and shows several examples of devices that can be used to transmit such data. Pet. 58 (citing Ex. 1007, 4:19–54; Ex. 1003 ¶¶ 141–157). For example, Petitioner asserts, *Beser* explains that the first and second network device each can be a cable modem. *Id.* (citing Ex. 1007, 4:30–42). Petitioner argues it was well known before February of 2000 that data transmitted via a cable modem inherently will be modulated, and that cable modems used various types of modulation, including FDM and TDM. *Id.* (citing Ex. 1003 ¶ 152). Petitioner also

asserts Beser explains that end devices can include portable VoIP devices such as mobile phones, and that data can be sent to and from such a device using data transmission standards that were developed by the Wireless Application Protocol (“WAP”) Forum. *Id.* (citing Ex. 1007, 4:43–63; Ex. 1003 ¶¶ 145–147). Petitioner argues that it was known in February 2000 that data transmitted to a mobile device using WAP could be transmitted over a cellular network, such as a GSM network (which employed TDM) or a CDMA network. *Id.* at 59 (citing Ex. 1003 ¶¶ 146–147; Ex. 1039).

With respect to claims 6, 7, 27, and 28, Patent Owner contends generally that “Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded that Petitioner has shown by a preponderance of the evidence that the combination of cited art teaches or suggests the recited limitations “wherein the telephony service uses modulation,” and “wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA),” of dependent claims 6, 7, 27, and 28.

e. Dependent Claims 8 and 29

Claims 8 and 29 depend from claims 1 and 22, respectively, and further specify that at least one of the first network device and the second network device is a “mobile device.” Petitioner asserts that Beser’s originating and terminating end devices can be “portable” devices. Pet. 59 (citing Ex. 1007, 4:50–52; Ex. 1003 ¶¶ 142, 145–147).

With respect to claims 8 and 29, Patent Owner contends generally that “Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31,

33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that Beser’s discussion of its originating and terminating end devices as portable devices teaches or suggests the limitation of a “wherein at least one of the first network device and the second network device is a mobile device,” recited by dependent claims 8 and 29.

f. Dependent Claims 9 and 30

Claims 9 and 30 depend from claims 1 and 22, respectively, and further specify that the identifier associated with the second network device is associated with a “*domain name*.” Petitioner asserts Beser’s tunneling request from the originating end device contains a unique identifier associated with the terminating end device. Pet. 59 (citing Ex. 1007, 8:1–3, 10:37–41; Ex. 1003 ¶ 173). Petitioner asserts Beser teaches many types of identifiers can be used for the unique identifier, and that in one preferred embodiment, the unique identifier is a domain name. *Id.* at 59–60 (citing Ex. 1007, 10:37–41; *see id.*, 10:37–11:8; Ex. 1003 ¶¶ 131, 174).

With respect to claims 9 and 30, Patent Owner contends generally that “Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that Beser’s tunneling request from the originating end device containing a unique identifier associated with the terminating end device and that in one embodiment the unique identifier is a domain name teaches or suggests the limitation “wherein the identifier associated with the second network device

is a domain name,” recited by dependent claims 9 and 30.

g. Dependent Claims 10 and 31

Claims 10 and 31 depend from claims 1 and 22, respectively, and further specify that “the established direct encrypted communication link supports data packets.” Petitioner asserts *Beser*, RFC 2401, and RFC 2543 all teach using IP packets. Pet. 60 (citing Ex. 1007, 7:6–26, 21:55–62; Ex. 1003 ¶ 134; Ex. 1008, 5–6; Ex. 1013, 58).

With respect to claims 10 and 31, Patent Owner contends generally that “*Beser* and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that the cited arts’ discussion of using IP packets teaches or suggests the limitation “wherein the established direct encrypted communication link supports data packets,” recited by dependent claims 10 and 31.

h. Dependent Claims 12 and 33

Claims 12 and 33 depend from claims 1 and 22, respectively, and further specify that “*determining that the second network device is available... is based at least in part on whether the second network device is authorized by the name service.*” Petitioner asserts *Beser* teaches that, in response to each VoIP request, the trusted-third-party network device evaluates the request and determines whether the unique identifier is listed in its internal database of registered users or devices. Pet. 60 (citing Ex. 1007, 11:30–36, 11:45–58; Ex. 1003 ¶¶ 177–178). Petitioner argues that if the terminating end device is registered as a subscriber, that is a determination that the device is authorized. *Id.* at 60–61 (citing Ex. 1003 ¶ 178).

With respect to claims 12 and 33, Patent Owner contends generally that “*Beser* and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that *Beser*’s discussion that, in response to each VoIP request, the trusted-third-party network device evaluates the request and determines whether the unique identifier is listed in its internal database of registered users or devices, and if the terminating end device is registered as a subscriber, that a determination is made that the device is authorized, teaches or suggests the limitation “wherein determining that the second network device is available to communicate through the established direct encrypted communication link is based at least in part on whether the second network device is authorized by the name service,” recited by dependent claims 12 and 33.

i. Dependent Claims 13 and 34

Claims 13 and 34 depend from claims 1 and 22, respectively, and further specify that “the data is encrypted along an entirety of the established direct encrypted communication link.”

Petitioner asserts *Beser* suggests encryption of audio and video, and a person of ordinary skill considering *Beser*’s IP tunneling scheme in view of RFC 2401 would have found it obvious to encrypt communications end-to-end. Pet. 61 (citing Ex. 1003 ¶¶ 231, 237). In the combined system, Petitioner argues, *Beser*’s IP tunnel would have provided anonymity for communications, and IPsec, as shown in Case 3 of RFC 2401, would have provided end-to-end encryption. *Id.* (citing Ex. 1008, 25; Ex. 1003 ¶¶ 233–237). With end-to-end encryption, Petitioner argues, data would be

encrypted along the entirety of the path between the originating and terminating devices. *Id.* (citing Ex. 1008, 25; Ex. 1007, Fig. 1).

Patent Owner argues Beser teaches away from using encryption, and therefore, Petitioner has failed to establish that claims 13 and 34 are unpatentable. PO Resp. 19–20 (citing PO Resp. Section III.D).

We disagree with Patent Owner that Beser teaches away from using encryption. As discussed above with regard to claim 1, Beser recognizes that encryption ordinarily should be used when the contents of a communication need to be protected. *See* Ex. 1007, 1:54–56. Beser also teaches using encryption when user-identifiable data are sent over a network, such as during establishment of an IP tunnel. *Id.* at 11:22–25. A person of ordinary skill in the art reading Beser would have understood that using encryption would help protect the contents of communications in an IP tunnel. *See* Ex. 1003 ¶¶ 233–241.

We are persuaded that Petitioner has shown by a preponderance of the evidence that the combination of Beser, RFC 2401, and RFC 2543 teaches or suggests the limitation “wherein the data is encrypted along an entirety of the established direct encrypted communication link between the first network device and the second network device,” recited by dependent claims 13 and 34.

j. Dependent Claims 14 and 35

Claims 14 and 35 depend from claims 1 and 22, respectively, and further specify that the request is received at another network device or processor that is “separate from the first network device.” Petitioner argues each of Beser’s first network device 14 and trusted-third-party device 30 “receives” the tunneling request (here, a VoIP request). Pet. 61–62 (citing

Ex. 1007, Figs. 1 & 6, 8:1–3, 8:21–47, 8:58–50, 9:46–49, 10:2–6; Ex. 1003 ¶¶ 171–72, 177). Petitioner argues each of first network device 24 and trusted-third-party device 30 are a “*device that is separate from the first network device* [originating device 24].” *Id.* at 62.

With respect to claims 14 and 35, Patent Owner contends generally that “Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that Beser’s discussion of transmitting a tunneling request between a first network device and a trusted-third-party device teaches or suggests the limitation “wherein the request is received and evaluated at another network device that is separate from the first network device,” recited by dependent claims 14 and 35.

k. Dependent Claims 15, 16, 36, and 37

Claims 15 and 36 depend from claims 1 and 22, respectively, and further specify that “the established direct encrypted communication link is a secure communication link.” Claims 16 and 37 depend from claims 1 and 22, respectively, and further specify that “the established direct encrypted communication link provides anonymity for at least one of the first network device or the second network device.”

Petitioner argues it would have been obvious to configure the Beser IP tunneling scheme to include end-to-end encryption of all IP traffic based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. Pet. 62 (citing Ex. 1003 ¶ 237; see Ex. 1008, 25). Petitioner argues that in the

combined system, Beser's IP tunneling technique would provide for anonymity for both the originating and terminating devices ("provides anonymity for at least one of the" devices). *Id.* at 62–63 (citing Ex. 1007, 12:13–19). Petitioner argues communications between the end devices are also both encrypted and anonymous, which satisfies the "secure communication link" element in this context. *Id.* at 63 (citing Ex. 1003 ¶ 80).

With respect to claims 15, 16, 36, and 37, Patent Owner contends generally that "Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend." PO Resp. 21.

We are persuaded by a preponderance of the evidence that the configuration of Beser's IP tunneling scheme to include end-to-end encryption of all IP traffic based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices providing for anonymity for both the originating and terminating devices teaches or suggests the recited limitations "wherein the established direct encrypted communication link is a secure communication link," and "wherein the established direct encrypted communication link provides anonymity for at least one of the first network device or the second network device," of dependent claims 15, 16, 36, and 37.

1. Dependent Claims 17 and 38

Claims 17 and 38 depend from claims 1 and 22, respectively, and further specify that "resolving the identifier associated with the second network device into the network address and returning the network address."

Petitioner argues that after Beser's trusted-third-party network device receives the VoIP request containing a unique identifier, it looks up the public IP address of the second network device associated with the identifier and the terminating device. Pet. 63 (citing Ex. 1007, 8:4–7, 11:26–32; 11:45–58). Petitioner asserts this address is returned to the first network device. *Id.* (citing Ex. 1007, 14:23–27; 14:19–33). Petitioner asserts that after the trusted-third-party network device obtains a private IP address for the terminating end device, it returns the address to the first network device and the originating device. *Id.* (citing Ex. 1007, 14:23–27, 21:38–42, 21:48–62). Thus, Petitioner argues, Beser shows the unique identifier is resolved into the network address for the terminating device and is returned. *Id.*

With respect to claims 17 and 38, Patent Owner contends generally that “Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that Beser's trusted-third-party network device looking up the public IP address of the second network device associated with the identifier and the terminating device and returning the address to the first network device and the originating device teaches or suggests the limitation “resolving the identifier associated with the second network device into the network address and returning the network address,” recited by dependent claims 17 and 38.

m. Dependent Claims 18 and 39

Claims 18 and 39 depend from claims 1 and 22, respectively, and further specify that “the network address is returned to the first network device.”

Petitioner asserts that after the VoIP request is processed by Beser's system, originating device 24 receives an IP address for terminating device 26. Pet. 64 (citing Ex. 1007, 21:48–62; Ex. 1003 ¶¶ 195–197).

With respect to claims 18 and 39, Patent Owner contends generally that “Beser and RFC 2401 do not render obvious claims 5–10, 12, 14–18, 26–31, 33, and 35–39 for at least the reasons discussed above for independent claims 1 and 22, from which they depend.” PO Resp. 21.

We are persuaded by a preponderance of the evidence that Beser's originating device 24 receiving an IP address for terminating device 26 after the VoIP request is processed by Beser's system, teaches or suggests the limitation “wherein the network address is returned to the first network device,” recited by dependent claims 18 and 39.

n. Dependent Claims 21 and 42

Claims 21 and 42 depend from claims 1 and 22, respectively, and further specify the steps of: “determining whether the first network device is authorized to communicate with the second network device” and “based on the determination that the second network device is available and that the first network device is authorized . . . , facilitating the establishment of the direct encrypted communication link.”

Petitioner asserts Beser explains that the request to initiate a VoIP association sent by the originating device may require encryption or authentication. Pet. 64 (citing Ex. 1007, 11:22–25). Petitioner argues that if the originating device is not authorized, the trusted-third-party network device would reject the request. *Id.* (citing Ex. 1003 ¶¶ 176–177). Thus, Petitioner argues, the trusted-third-party network device will only proceed to facilitate a secure connection if it determines the originating device is

authorized and if it determines the terminating device is available. *Id.* at 64–65.

Patent Owner argues that Beser is completely silent on any determination regarding the authorization of the first network device to communicate with the second network device. PO Resp. 20–21 (citing Ex. 1007, 11:22–25). Patent Owner argues that Dr. Tamassia’s declaration is silent regarding any determination that the first network device is authorized to communicate with the second network device. *Id.* (citing Ex. 1003 at ¶¶ 176–77). The mere disclosure of a tunneling request being “authenticated,” Patent Owner argues, is simply insufficient to disclose the claimed determination. *Id.* at 21.

Patent Owner’s argument is not persuasive. Beser’s trusted-third-party network device, as modified by the RFC documents to include encryption as explained above, would be able to decrypt and authenticate the received request to determine whether to grant the tunneling request, where Beser teaches encryption and authentication techniques were well-known, and Beser also discloses using encryption of packet portions and/or authentication thereof for security reasons. *See* Ex. 1003 ¶¶ 176–178; Ex. 1007, 11:22–25. In further processing the request, the unique identifier is compared with a database that includes authorized users or devices. Ex. 1003 ¶ 178; *see also* Ex. 1007, 11:48–52. Based on the decryption, authentication, and comparison, the trusted-third-party network device grants or denies (i.e., authorizes) establishing and negotiating a secure connection between the first and second network device. Ex. 1003 ¶¶ 176–177. Moreover, the ’163 patent explains that authorization can be determined in numerous ways, including by checking a list, “communicating

with” a gatekeeper, or “transmitting a request message back to the user’s computer.” Ex. 1001, 41:14–27. Beser’s process of determining whether to grant a tunneling request by comparing a unique identifier with a database that includes authorized users and devices before establishing a secure connection between a first and second network device is an example of “checking a list” to determine authorization.

We are persuaded by a preponderance of the evidence that Beser’s trusted-third-party network device, as modified, includes decrypting and authenticating a received request to determine whether to grant a tunneling request, then comparing the unique identifier with a database that includes authorized users or devices, and granting or denying establishing and negotiating a secure connection between the first and second network device, thereby teaching or suggesting the limitation “determining whether the first network device is authorized to communicate with the second network device through the direct encrypted communication link,” recited by dependent claims 21 and 42.

3. Public Accessibility of RFC 2401(Ex. 1008) and RFC 2543 (Ex. 1013)⁴

Petitioner contends that RFC 2401 (Ex. 1008) and RFC 2543 (Ex. 1013) were published by the Internet Engineering Task Force (IETF) in November 1998 and March 1999, respectively, and are prior art to the ’163 patent under 35 U.S.C. § 102(b). Pet 24, 28 (citing Ex. 1008, 1; Ex. 1013, 1; Ex. 1003 ¶¶ 125–128). Petitioner asserts that the documents list November

⁴ In an earlier proceeding, IPR2016-00332, the Board found RFC 2401 and RFC 2543 were prior art printed publications to U.S. Patent No. 8,504,696. See IPR2016-00332, Paper 29, at 48-52 (June 22, 2017).

1998 and March 1999, respectively, as their publication date, and are marked with “Distribution of this memo is unlimited” on their covers. *Id.* (citing Ex. 1008, 1; Ex. 1013, 1). Further, Petitioner argues, RFC 2026 (Ex. 1036), which describes the IETF’s publication practices, explains that RFCs can be obtained from a number of Internet hosts using anonymous FTP, gopher, WWW, and other document-retrieval systems. *Id.* (citing Ex. 1036, 3, 5; Ex. 1003 ¶¶ 117–124). Petitioner explains that RFCs are “debated in open meetings and/or public electronic mailing lists, and [are] made available for review via world-wide on-line directories.” *Id.* at 24 (citing Ex. 1036, 3; Ex. 1008, 1; Ex. 1003 ¶¶ 118–120).

Petitioner argues that one of ordinary skill in the art would have been aware of the IETF’s publication practices, and would have known how to obtain RFC publications because of their wide distribution and importance to the Internet community as a whole. *Id.* (citing Ex. 1003 ¶¶ 122–124). For example, Petitioner asserts, Beser notes that “IETF standards can be found at the URL ‘www.ietf.org.’” *Id.* (citing Ex. 1007, 4:67–5:1). Petitioner notes that a number of industry publications published prior to February 2000 explicitly reference RFC 2401 and state that RFC 2401 could be downloaded from the IETF. *Id.* at 24–25 (citing Ex. 1064, 9; Ex. 1065, 3). Finally, Petitioner asserts, the full text of RFC 2401 was included in the book *Implementing IPsec* (submitted as Exhibit 1072), published in 1999, that describes the IPsec protocol and compiles the relevant RFCs. *Id.* at 25; see also Ex. 1073 (U.S. Copyright Registration form for Ex. 1072).

Moreover, Petitioner argues, the IETF confirmed RFC 2401’s publication date through testimony by Sandy Ginoza, acting as a designated representative of IETF, during proceedings in a related matter between

Petitioner and Patent Owner. *Id.* (citing Ex. 1060 ¶¶ 1–5; Ex. 1063, 6:23–7:4; *id.* at 10:5–11:22). Ms. Ginoza, Petitioner explains, testified that the “RFC Editor maintained a copy of RFC 2401 in the ordinary course of its regularly conducted activities” and that RFC 2401 was published and “has been publicly available through the RFC Editor’s web site or through other means since its publication in November 1998.” *Id.* (citing Ex. 1060 ¶ 107; *id.* at ¶¶ 105–107). Petitioner points out that in a deposition about her declaration, Ms. Ginoza testified that RFC 2401 was made publicly available in “November 1998.” *Id.* (citing Ex. 1063, 39:14–40:24; Ex. 1062. Ms. Ginoza also testified that RFC 2543 was published on March 1999. *Id.* at 28 (citing Ex. 1060 ¶¶ 168–170; Ex. 1063, 45:5–46:17).

Patent Owner argues that Petitioner’s assertion that the RFCs were published by the date on their covers is insufficient to establish that a reference qualifies as a printed publication. PO Resp. 22–23. Patent Owner also argues that Dr. Tamassia’s testimony does not constitute sufficient evidence because it has not been established that Dr. Tamassia has personal knowledge that the RFCs were released to the public or that Dr. Tamassia is familiar with the workings of the IETF. *Id.* at 23–24.

Patent Owner also argues that Ms. Ginoza does not have any personal knowledge of when the RFCs became publicly available and Ms. Ginoza has not provided the underlying facts or data on which her opinion is based. *Id.* at 25–26. Patent Owner argues that the procedures described in RFC 2026 are meant to be “flexible” and reflect “generally-accepted practices,” and there is no assurance that the procedures of RFC 2026 that were quoted by Petitioner were actually applied to the RFCs. *Id.* at 27. Patent Owner argues that the notation that “Distribution of this memo is unlimited” on the cover

pages of the RFCs does not indicate that the RFCs were “*actually* . . . released or distributed to the public” to meet the requirement of public accessibility. *Id.* at 27–28.

“A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

Here, the evidence supports a finding that persons interested and ordinarily skilled in the subject matter of RFC 2401 and RFC 2543 could have located them. RFC 2401 and RFC 2543 each include dates on each page, and the cover sheets bear the designations “Request for Comments” from the “Network Working Group,” discussing particular standardized protocols for the Internet. Ex. 1008, 1; Ex. 1013, 1. Each document describes itself as a “document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements Distribution of this memo is unlimited.” See Ex. 1008, 1; Ex. 1013, 1.

Ms. Ginoza, a representative of IETF, states in her declaration that “RFC 2401 has been publicly available through the RFC Editor’s web site or through other means since its publication in November 1998.” Ex. 1060 ¶ 107. Ms. Ginoza also states that “RFC 2543 has been publicly available through the RFC Editor’s web site or through other means since its publication in March 1999.” Ex. 1060 ¶ 170. Patent Owner’s criticism of

Ms. Ginoza's testimony as lacking personal knowledge is not persuasive. Ms. Ginoza testified as an IETF corporate representative. See Ex. 1060 ("Declaration of the RFC Publisher for the Internet Engineering Task Force, an Organized Activity of the Internet Society"). It is well established that corporate representatives "need not have first-hand knowledge of the events in question" so long as they are "adequately prepared" to answer on behalf of the corporation. See *United States v. Taylor*, 166 F.R.D. 356, 361 (M.D.N.C. 1996), *aff'd*, 166 F.R.D. 367 (M.D.N.C. 1996). Patent Owner's criticism that Ms. Ginoza did not provide the basis for her "opinion" is also misplaced. Ms. Ginoza was not providing an expert opinion; she was a corporate representative of IETF testifying as to certain facts concerning the RFC Series of documents. *Id.* ¶¶ 1–5.

Dr. Tamassia testifies that RFCs are "prepared and distributed under a formalized publication process overseen by one of several Internet standards or governing bodies," such as the IETF. Ex. 1003 ¶ 117. Dr. Tamassia also relies on an RFC publication that discusses the RFC development and publication process itself—RFC 2026, dated October 1996. *Id.* ¶¶ 118–124. Dr. Tamassia states that "[t]he publication date of each RFC is contained in the RFC, typically in the top right corner of the first page of the document" and "[t]his is the date it was released for public distribution on the Internet." *Id.* ¶ 121 (citing Ex. 1036, 20). Dr. Tamassia quotes RFC 2026, which explains that anyone can obtain RFCs from "a number of Internet hosts," making the "working document readily available to a wide audience, facilitating the process of review and revision." Ex. 1003 ¶ 120 (quoting Ex. 1036, 8).

We find Ms. Ginoza's and Dr. Tamassia's testimony as to public

accessibility of RFCs in general to be credible, especially given the independent support of RFC 2026 (Ex. 1036). The contents of RFC 2401 and 2543 are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including the requests for discussion and suggestions for improvements in each document, and the dates “November 1998” and “March 1999” respectively on the top right corner of the first page of each document. *See* Ex. 1008, 1; Ex. 1013, 1. This is consistent with Ms. Ginoza’s testimony that RFC 2401 and RFC 2543 have been publicly available through the RFC Editor’s web site or through other means since their publication in November 1998 and March 1999, respectively. Ex. 1060 ¶¶ 107, 170.

The title itself on each document, “Request for Comments,” coupled with evidence in RFC 2026 that each RFC document was made widely available “from a number of Internet hosts,” constitutes sufficient evidence that RFC 2401 and 2543 each was intended for publication and would have been accessible to interested artisans seeking documents related to “Internet standards.” Ex. 1036, 6, 8; Ex. 1008, 1; Ex. 1013, 1; Ex. 1003 ¶¶ 187–89; Ex. 1060 ¶¶ 107, 170. In other words, these documents—each a request for suggestions and improvements for Internet standards and having no indication of being a mere draft or internal paper—are precisely the type of documents whose main purpose is for public disclosure.

Petitioner provides additional documentary evidence, in the form of an August 16, 1999 Info World magazine article (Ex. 1064, 9 (discussing RFC 2401 and IPsec protocols and stating “[a]ll of these documents are available on the IETF website”)), and an article from Network World magazine (dated March 15, 1999) (Ex. 1065), which sets forth an imperative

statement: “See the IETF documents RFC 2401 . . . at www.ietf.org/rfc/rfc2411.text.” Ex. 1065, 3. Both of the magazine articles, Exhibits 1064 and 1065, further corroborate the indicia of availability, although they are not necessary to our finding of public accessibility.

We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401(dated November 1998) and RFC 2543 (dated March 1999) were made available to persons of ordinary skill interested in computer networking and security sufficiently to be deemed “publicly accessible” at the relevant time. Therefore, we determine RFC 2401 and RFC 2543 qualify as prior art printed publications.

E. Patent Owner’s Motion to Exclude

Patent Owner moves to exclude exhibits 1008, 1013, 1032–1036, 1038–1040, 1045–1048, 1053, 1060, 1063–1065, and 1072–1074, at least in part, because these exhibits allegedly include inadmissible hearsay. Paper 23, 1. Patent Owner acknowledges, however, “the Board has previously found unpersuasive arguments similar to some of the arguments set forth in this motion. *See, e.g.,* IPR2016-00331, Paper No. 29.” *Id.* at 1 n.1.

Petitioner notes that “[i]n Final Written Decisions involving the same exhibits at issue here, the Board considered and found unpersuasive or irrelevant many of the same arguments that Patent Owner now advances. *See* IPR2016-00331, Paper 29, 46–48 (June 22, 2017); IPR2015-00810, Paper 44, 56–57 (Aug. 30, 2016); IPR2015-00811, Paper 44, 68–71 (Sept. 8, 2016); IPR2015-00812, Paper 43, 40–41 (Aug. 30, 2016); IPR2015-00871,

Paper 39, 73–77 (Sept. 28, 2016); IPR2016-00331, Paper 29, 46–49 (June 22, 2017); IPR2016-00332, Paper 29, 80–85 (June 22, 2017).” Paper 26, 1.⁵

1. Exhibits 1008 and 1013

Patent Owner argues that Petitioner relies on the text, “November 1998,” on the cover of Exhibit 1008 and “March 1999,” on the cover of Exhibit 1013 for the truth of the matter asserted. Paper 23, 2. Therefore, Patent Owner argues, these portions of Exhibits 1008 and 1013 constitute inadmissible hearsay and should be excluded. *Id.* Petitioner argues Exhibits 1008 and 1013 are admissible under the business records exception. Paper 26, 4–7.

The business records exception to the rule against hearsay applies if “the record was kept in the course of a regularly conducted activity of ... [an] organization... [and] making the record was a regular practice of that activity.” FRE 803(6)(B)-(C). In addition, the record must be “made at or near the time by . . . someone with knowledge.” FRE 803(6)(A).

Both Dr. Tamassia and RFC 2026 (Ex. 1036) explain that publishing RFCs were part of IETF’s standard process to “provide[] ample opportunity for participation and comment by all interested parties.” Ex. 1036, 4; Ex. 1003 ¶¶ 118–123. Dr. Tamassia testifies that IETF regularly specifies a publication date on the top right corner of each RFC—here, “November 1998” at the top of RFC 2401 and “March 1999” at the top of RFC 2543—to establish response deadlines for comments. Ex. 1003 ¶¶ 117–124, 126, 128.

⁵ Our reviewing court recently affirmed the Board’s final decisions in IPR2015-00810, IPR2015-00811, IPR2015-00812, IPR2015-00866, IPR2015-00868, IPR2015-00870, and IPR2015-00871, in *Virentx, Inc. v. Apple, Inc.*, 715 F. App’x 1024 (Fed. Cir. 2018) (Fed. Cir. R. 36).

Ms. Ginoza’s prior testimony corroborates Dr. Tamassia’s testimony with respect to RFC 2401 and RFC 2543. She testified that RFC 2401 and RFC 2543 were kept in the ordinary course of IETF’s regularly conducted activities and “been publicly available through the RFC Editor’s website or through other means since [their] publication” on their respective dates—i.e., “November 1998” for RFC 2401 and “March 1999” for RFC 2543. Ex. 1060 ¶¶ 105–107, 168–70; Ex. 1063, 39:14–40:24.

Alternatively, the dates on Exhibit 1008 and Exhibit 1013 do not constitute hearsay, because they are not assertions that IETF published RFC 2401 or RFC 2543 on a certain date. *See Seabery N. Am. Inc. v. Lincoln Glob., Inc.*, Case IPR2016-00840, slip. op. at 5–6 (PTAB Oct. 2, 2017) (Paper 60, 5–6 & n.2) (reasoning dates do not constitute hearsay because they are not assertions) (quoted below).

With further respect to Exhibit 1008, RFC 2401, in addition to a Copyright Notice” of “1998,” title (“Security Architecture for the Internet Protocol”), and table of contents, it bears the following date and other identifying information on the first page:

Network Working Group
Request for Comments: 2401
Obsoletes: 1825
Category: Standards Track

S. Kent
BBN Corp
R. Atkinson
@Home Network
November 1998

Ex. 1008, 1.

Similar information appears on the first page of Exhibit 1013, RFC 2543 (date “March 1999”). Ex. 1013, 1. All of this information serves to identify and authenticate each document.

Regarding hearsay, in *Seabery*, the Board reasoned as follows:

We agree with the view [of other PTAB panels] that the dates [of publications] are not hearsay because they are not assertions. . . . We are supported in this by cases such as *United States v. Snow*, 517 F.2d 441, 445 (9th Cir. 1975), where a red tape bearing the defendant's name affixed to a briefcase where a gun was found was admitted as circumstantial evidence that the defendant possessed the weapon. To the same effect are *United States v. Koch*, 625 F.3d 470, 480 (8th Cir. 2010) (computer flash drive with manufacturer's label "China" not inadmissible hearsay to prove place of manufacture); and *United States v. Bowling*, 32 F.3d 326, 328 (8th Cir. 1994) (manufacturer's name stamped on firearm not hearsay). We are persuaded by these cases that dates appearing in Exhibit 1003, like the examples in those cases, are circumstantial evidence of publication and not assertions that publication occurred on a date certain. We, therefore, overrule the objection and admit the dates for this purpose.

See IPR2016-00840, Paper 60, 5–6 & n.2 (alternatively relying on the residual exception to hearsay). For the same reasons enunciated in *Seabery*, Patent Owner does not establish that the dates ("November 1998" and "March 1999") constitute hearsay, because these dates are not assertions of a publication. Rather, they constitute evidence helping to identify the documents and include circumstantial evidence that IEFT made the RFC 2401 and RFC 2543 publications available respectively in November 1998 and March 1999. The following notices, "Copyright Notice" and "Copyright (C) The Internet Society (1998). All Rights Reserved," on the RFC 2401 document, with similar notation on the RFC 2543 document, provides further corroboration and circumstantial evidence of the date and authenticity. See Ex. 1008, 1.

Petitioner also shows, in the alternative, that Exhibits 1008 and 1013 satisfy Fed. R. Evid. 807(a) under the residual exception to hearsay. Paper 26, 8–15. We adopt Petitioner's showing as persuasive. See *id.*

Based on the above-discussed evidence, Exhibits 1008 and 1013 qualify under the business records or residual exceptions to the rule against hearsay, or the dates do not constitute hearsay. Patent Owner fails to show that the publication date or its source—i.e., RFC 2401 and RFC 2543—indicate a lack of trustworthiness, as required under FRE 803(6)(E). Patent Owner’s motion to exclude Exhibits 1008 and 1013 on hearsay grounds is denied.

2. Exhibits 1032–36

Patent Owner argues that Petitioner relies on the dates stamped on Exhibits 1032–35 to establish that the content contained within the exhibits reflects the knowledge in the art “prior to the ’163 patent’s effective date” is a hearsay purpose because it relies on the truth of the dates. Paper 32, 2–3. Regarding Exhibit 1036, Patent Owner argues that Petitioner relied upon this exhibit solely for the truth of the RFC publication practices purportedly disclosed within—a hearsay purpose. *Id.* at 3.

Petitioner argues Exhibits 1032–36 serve a non-hearsay purpose. Paper 26, 2. Petitioner asserts reliance on Exhibits 1032–35 to show “technologies described in the ’163 patent, including DNS servers, domain names, and VPNs, were well-known in the art prior to the ’163 patent’s effective filing date.” *Id.*, Pet. 4 (citing Ex. 1032–1035). Exhibit 1036 shows that one of ordinary skill in the art would have been aware of the IETF’s publication practices, and would have known how to obtain RFC publications. Pet. 24.

The Board has held previously that a statement is not hearsay if offered for the effect the statement had on the understanding of a person of ordinary skill in the art, or “to show what one of ordinary skill in the art

would have known about the technical features and developments in the pertinent art.” *See Apple v. DSS Tech. Mgmt.*, IPR2015-00369, Paper 40 at 38 (June 17, 2016); *Liberty Mut. Ins. Co. v. Progressive Cas. Ins.*, CBM2012-00010, Paper 59 at 36–37 (Feb. 14, 2014).

Here, Petitioner relies on Exhibits 1032–35 to show that technologies described in the ’163 patent, including DNS servers, domain names, and VPNs, were well-known in the art prior to the ’163 patent’s effective filing date. *See* Pet. 4. Exhibit 1036 shows that one of ordinary skill in the art would have been aware of the IETF’s publication practices, and would have known how to obtain RFC publications. Pet. 24. Such uses are for non-hearsay purposes. Accordingly, Patent Owner’s motion to exclude Exhibits 1032–36 on hearsay grounds is denied.

3. Exhibits 1038–40, 1045–48, 1053, and 1074

Patent Owner argues that Petitioner’s expert relies on Exhibits 1038–40, 1045–48, 1053, and 1074 for the purported truth of the matters asserted in these documents, and that they should therefore be excluded as inadmissible hearsay. Paper 23, 3.

As a threshold issue, Patent Owner’s motion with respect to Exhibits 1038–40, 1045–48, 1053, and 1074 fails to satisfy its burden of proof because Patent Owner does not identify specifically what statements in these exhibits are hearsay. *See* Paper 23, 3; 37 C.F.R. § 42.20(c); IPR2016-00331, Paper 29 at 47 (“Patent Owner does not explain why [the exhibits] are hearsay or what part of them constitute hearsay.”). Patent Owner merely states “Petitioner’s expert relies on [the exhibits] for the purported truth of the matters asserted” and cites large swaths of the Petition and Petitioner’s expert declaration. Paper 23, 3. Patent Owner “does not identify

specifically the textual portions of the aforementioned exhibits that allegedly are being offered for the truth of the matter asserted, yet seeks to exclude the entirety of each exhibit.” *Liberty Mut. Ins.*, CBM 2012-00010, Paper 59 at 36. The Board will not “go through the entirety of each exhibit and determine which portion of the exhibit [Patent Owner] believes to be hearsay.” *Id.*

Patent Owner’s failure to identify the allegedly hearsay statements is sufficient reason alone to deny its motion to exclude Exhibits 1038–40, 1045–48, 1053, and 1074.

4. *Exhibits 1060, 1063–65, and 1072–73*⁶

Patent Owner argues that, “[e]ach of Exhibits 1060, 1063–65, and 1072–73 include out-of-court statements. Paper 23, 4. Patent Owner argues Petitioner relies on the alleged truth of these out-of-court statements, making them inadmissible hearsay. *Id.*

Regarding Exhibits 1060 and 1063, Patent Owner argues Petitioner relies on these exhibits solely for the purported truth of the RFC’s publication date and IETF business practices as asserted by Ms. Ginoza. *Id.* at 4–5. Regarding Exhibits 1064 and 1065, Patent Owner argues that Petitioner relies on these exhibits to support its assertion that “[a] number of industry publications published prior to February 2000 explicitly reference RFC 2401 and state that RFC 2401 could be downloaded from the IETF.” *Id.* at 5 (quoting Pet. 24–25).

Regarding Exhibit 1072, Patent Owner argues Petitioner’s reliance on

⁶ Patent Owner acknowledges that the Board admitted Exhibits 1060 and 1063–65 under the residual exception set forth in Rule 807 in a related proceeding. Paper 23, 7; see IPR2016-00331, Paper No. 29.

the date printed on that reference for the assertion that Exhibit 1072 was “published in 1999” is hearsay. *Id.* at 6 (quoting Pet. 26). Similarly, Patent Owner argues Petitioner presents Exhibit 1073 solely for the improper hearsay purpose of supporting its assertion that Exhibit 1072 was “published in 1999.” *Id.*

Federal Rule of Evidence 807(a) states that a “statement is not excluded by the rule against hearsay” if “(1) the statement has equivalent circumstantial guarantees of trustworthiness; (2) it is offered as evidence of a material fact; (3) it is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts; and (4) admitting it will best serve the purposes of these rules and the interests of justice.”

Exhibits 1060 and 1063 contain the testimony of Ms. Sandy Ginoza; Exhibit 1064 is an InfoWorld magazine article from 1999; Exhibit 1065 is a NetworkWorld magazine article from 1999; and Exhibit 1072 is a book entitled Implementing IPsec from 1999. Petitioner relies on RFC 2401 and RFC 2543 as prior art printed publications. Petitioner relies on Exhibits 1060, 1063–65, and 1072 to corroborate RFC 2401’s public availability and distribution via the Internet prior to February 2000. Pet. 24–25; Pet. Reply, 19–22. Similarly, Petitioner relies on Exhibits 1060 and 1063 to corroborate RFC 2543’s public availability and distribution prior to February 2000. Pet. 28; Pet. Reply, 19–22. The Board previously found that Exhibits 1064 and 1065 satisfy the residual hearsay exception (and dismissed as moot challenges to Exhibits 1060 and 1063). *See* IPR2016-00331, Paper 29 at 48.

Exhibits 1060, 1063–65, and 1072 have equivalent circumstantial guarantees of trustworthiness. Exhibits 1060 and 1063 contain the prior

sworn testimony of Ms. Ginoza and IETF and reflect Patent Owner's cross-examination of Ms. Ginoza on the substance of her testimony. Exhibit 1060 is a declaration from Sandy Ginoza, acting as a designated representative of the IETF, created in response to a subpoena served as part of an investigation initiated by Patent Owner before the International Trade Commission (337-TA-858). Ex. 1060 ¶¶ 1–5; Ex. 1063, 6:23–7:4, 10:5–14.

In her declaration, Ms. Ginoza testified that RFC 2401 and RFC 2543 were published on the RFC Editor's website and were publicly available before February 2000. Ex. 1060 ¶¶ 105–107, 168–170. Exhibit 1063 is the transcript of Ms. Ginoza's February 8, 2013 deposition that was taken as part of the ITC action, where she testified that both RFC 2401 and RFC 2543 were publicly available prior to February 2000. Ex. 1063, 39:14–24, 45:5–46:17; *see id.* at 10:5–11:22 (confirming her knowledge of IETF publishing practices as they relate to RFCs). Patent Owner cross-examined Ms. Ginoza about her testimony and declaration, but developed no contrary testimony. *See id.* at 50:16–69:1.

This evidence is corroborated by and corroborates the disclosure in Exhibits 1064 and 1065, which are excerpts from industry publications predating February 2000 that state it was known that RFCs—and RFC 2401 specifically—were publicly available through the Internet, including through the IETF's website. *See, e.g.*, Ex. 1064 at 9 (discussing RFCs 2401 to 2408 and stating “[a]ll of these documents are available on the IETF website: www.ietf.org/rfc.html”); Ex. 1065 at 3 (discussing IP security protocols and stating “[s]ee the IETF documents RFC 2401 ‘Security Architecture for the Internet Protocol’ at www.ietf.org/rfc/rfc2401.txt”).

Further, Exhibit 1072 is corroborated by and corroborates Exhibits

1008, 1060, 1063–65 in showing RFC 2401 was publicly available. By being published before February 2000, Exhibit 1072 shows that RFC 2401 was publicly available by providing the full text of RFC 2401 in its appendix. Pet. 25; see Ex. 1072 at 173–240.

Exhibits 1060, 1063–65, and 1072 are offered as evidence of a material fact: the public availability of RFC 2401 and RFC 2543 prior to February 2000. Pet., 24–25, 28. It would be in the interest of justice to admit Exhibits 1060, 1063–1065, and 1072, because RFC documents, such as those at issue here, are well-known sources of technical information in the art at issue in this proceeding. Excluding Ms. Ginoza’s testimony about these documents—particularly where Patent Owner has already cross-examined her on that testimony—would not comport with “an administrative proceeding designed and intended to afford expedited and efficient relief.” See *Ericsson Inc. v. Intellectual Ventures I LLC*, IPR2014-00527, Paper 41 at 12 (May 18, 2015). Likewise, Exhibits 1064, 1065, and 1072 are journal articles and books from publications that were well-known to those of skill, and their exclusion would remove a reliable source of evidence from the record.

Exhibits 1060, 1063–65, and 1072 satisfy the requirements of the residual exception to the rule against hearsay. Exhibit 1073 is an admissible public record from the United States Copyright Office. Therefore, Patent Owner’s motion to exclude Exhibits 1060, 1063–65, 1072, and 1073 is denied.

III. CONCLUSION

Based on all the evidence of record, we determine that Petitioner has established by a preponderance of the evidence that claims 1–10, 12–18, 21–31, 33–39, and 42 of the '163 patent would have been obvious under 35 U.S.C. § 103(a) over the combined teachings of Beser, RFC 2401, and RFC 2543.

IV. ORDER

For the reasons given, it is

ORDERED that claims 1–10, 12–18, 21–31, 33–39, and 42 of the '163 patent are unpatentable; and

FURTHER ORDERED that Petitioner's Motion to Exclude is denied; and

FURTHER ORDERED that parties to the proceeding seeking judicial review of the Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2017-00337
Patent 9,038,163 B2

PETITIONER:

Jeffrey P. Kushan
Thomas A. Broughan, III
SIDLEY AUSTIN LLP
jkushan@sidley.com
tbroughan@sidley.com

PATENT OWNER:

Joseph E. Palys
Naveen Modi
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com