

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00870
Patent 8,560,705 B2

Before KARL D. EASTHOM, JENNIFER S. BISK, and
GREGG I. ANDERSON, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*.

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

I. INTRODUCTION

Petitioner, Apple Inc., filed a Petition (Paper 1, “Pet.”) seeking an *inter partes* review of claims 1–30 of U.S. Patent No. 8,560,705 B2 (Ex. 1050, “the ’705 patent”) pursuant to 35 U.S.C. §§ 311–319. After VirnetX Inc., Patent Owner, filed a Preliminary Response (Paper 6), we instituted an *inter partes* review of claims 1–30 (Paper 8, “Institution Decision” or “Inst. Dec.”).

Subsequent to institution, Patent Owner filed a Patent Owner Response (Paper 23) (“PO Resp.”), and Petitioner filed a Reply (Paper 26) (“Pet. Reply”). Patent Owner also filed a Motion to Exclude evidence (Paper 30), Petitioner filed an Opposition (Paper 33), and Patent Owner filed a Reply to the Opposition (Paper 34). Petitioner relies on, *inter alia*, the “Declaration of Roberto Tamassia Regarding U.S. Patent Nos. 8,458,341, 8,516,131, and 8,560,705.” Ex. 1005 (the “Tamassia Declaration”). Patent Owner relies on, *inter alia*, the “Declaration of Fabian Monroe, Ph.D.” Ex. 2018 (the “Monroe Declaration”). The Board filed a transcription of the Oral Hearing held on June 27, 2016. Paper 38. This Final Written Decision issues concurrently with the final written decision involving the ’705 patent in *Apple Inc. v. VirnetX Inc.*, IPR2015-00871 (PTAB Sept. 28, 2016) (Paper No. 39, “’871 FWD”) (generally “’871 IPR”).

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–30 of the ’705 patent are unpatentable.

A. The '705 Patent (Ex. 1050)

The '705 patent describes secure methods for communicating over the Internet. Ex. 1050, 9:41–46. Specifically, the '705 patent describes “the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.” *Id.* at 39:4–6. This automatic creation employs a modified Domain Name Server, which may include a conventional Domain Name Server (DNS):

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name “Yahoo.com,” the user’s web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user’s browser and then used by the browser to contact the destination web site.

Id. at 39:7–13.

“A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610,” which may be “combined into a single server for convenience.” *Id.* at 39:67–40:2, 40:45–46. The DNS proxy of the modified DNS server intercepts all DNS lookup requests, determines whether the user has requested access to a secure site (using, for example, a domain name extension or an internal table of secure sites), and if so, determines whether the user has sufficient security privileges to access the requested site. *Id.* at 40:6–16. If the user has requested access to a secure site to which it has insufficient security privileges, the DNS proxy returns a “‘host unknown’” error to the user. *Id.* at 40:32–33. If the user has requested access to a secure site to which it has sufficient security privileges, the DNS proxy requests a gatekeeper to create a VPN between the user’s computer and the secure target site. *Id.* at 40:12–16. The DNS proxy then

returns to the user the resolved address passed to it by the gatekeeper, which need not be the actual address of the destination computer. *Id.* at 40:19–25.

The VPN is “preferably implemented using the IP address ‘hopping’ features,” (changing IP addresses based upon an agreed upon algorithm) described elsewhere in the ’705 patent, “such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted.” *Id.* at 39:52–56. The system may hide the identities (i.e., anonymity, a form of security) by encrypting parts of packets. *See id.* at 1:50–56, 9:41–10:17. Routers along the hopping path determine the “next-hop in a series of . . . router hops” (*id.* at 9:52–53) in the path, by authenticating or decrypting transmitted encrypted parts of packets to find the “next-hop” router address. *See id.* at 3:23–25, 10:2–17. Data messages in the packets also may be encrypted. *See id.* at 1:50–56, 4:10–12, 11:1–9.

B. Illustrative Challenged Claim

Claims 1 and 16 of the ’705 patent are independent and of similar scope. Claim 1, illustrative of the challenged claims, follows:

1. A client device comprising:
 - (a) memory configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on
 - (i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device, and
 - (ii) a determination as a result of the request that the target device is a device with which a secure communication link can be established;

- (b) an application program configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established; and
- (c) a signal processing configuration arranged to execute the application program.

Ex. 1050, 55:52–65.

C. Instituted Grounds of Unpatentability

We instituted on the following grounds asserted by Petitioner under 35 U.S.C. § 103 for obviousness: claims 1–23 and 25–30 of the '705 patent based on the combination of Beser (Ex. 1007)¹ and RFC 2401 (Ex. 1008)², and claim 24 as unpatentable based on the combination of Beser, RFC 2401, and Brand (Ex. 1012)³. Inst. Dec. 19.

D. Claim Construction

In an *inter partes* review, the Board construes claim terms in an unexpired patent under their broadest reasonable construction in light of the specification of the patent in which they appear. *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016); 37 C.F.R. § 42.100(b). Under this standard, absent any special definitions, claim terms or phrases carry their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

The Board construed similar claim terms in *Apple Inc. v. VirnetX Inc.*, IPR2014-00237 (PTAB May 11, 2015) (Paper 41) (“’237 final written

¹ U.S. Patent No. 6,496,867 B1.

² S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998.

³ U.S. Patent No. 5,237,566.

decision,” “’237 FWD,” or generally, “’237 IPR”) (on appeal at the Federal Circuit) and in *Apple Inc. v. VirnetX Inc.*, IPR2014-00481 (PTAB Aug. 24, 2015) (Paper 35) (“’481 final written decision,” “’481 FWD,” or generally, “’481 IPR”) (on appeal at the Federal Circuit). *See also VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents having similar claim terms).

1. Interception of a Request—Claims 1 and 16

In the related ’237 IPR, as Petitioner and Patent Owner note, we construed the similar phrase “intercepting a request” as “receiving a request pertaining to a first entity at another entity.” ’237 FWD 10–12; PO Resp. 4; Pet. 8–10. Quoting Patent Owner in that proceeding, we noted that Patent Owner “disagrees with this construction” (’237 PO Resp. 23), but “believes that no construction is necessary” (*id.* at 26), because “it does not appear that the construction of ‘intercepting’ will bear on the outcome of the issues in this *inter partes* review” (*id.* at 23). ’237 FWD 11. The ’237 IPR and this proceeding involve the same issue with respect to this term and the asserted prior art.

Patent Owner similarly states in the instant proceeding that “[n]o construction [is] necessary.” PO Resp. 4. Nevertheless, as it did in the ’237 IPR, Patent Owner urges that if we construe the term, then we adopt Patent Owner’s construction: “receiving a request to look up an internet protocol address and, apart from resolving it into an address, preforming an evaluation on it related to establishing a secure communication link.” PO Resp. 4; ’237 PO Resp. 23.

According to Patent Owner’s argument in the ’237 IPR, a disclosed modified DNS “appl[ies] an additional layer of functionality to a request to

look up a network address beyond merely resolving it and returning the network address.” *Id.* at 25. Patent Owner’s arguments here are similar. For example, Patent Owner argues that its “alternative construction appropriately captures the notion of performing an additional evaluation on a request to look up an IP address related to establishing an encrypted communications channel, beyond conventionally resolving it and returning the address.” PO Resp. 4–5.⁴

Both the arguments and record show that Patent Owner’s proposed construction adds unnecessary functionality to “intercepting a request” and violates the plain language of the claim. According to Patent Owner’s arguments, another recited phrase in claim 1 (and a similar phrase in claim 16), captures the functionality, in particular, the “determination” clause of claim 1. *See* PO Resp. 5 (listing one example function to be incorporated as “determin[ing] that a device [] is available for the secure communication service”). In other words, the “determination” clause already covers functionality that Patent Owner urges is implicit in the intercepting phrase. *See* PO Resp. 4–5; Prelim. Resp. 31–32; ’237 PO Resp. 26, 29–30.

The parties agree that “interception of a request” (at least) involves “receiving a request” at some intermediate device. PO Resp. 4; Pet. 9–10. Patent Owner’s proposed construction does not create any distinction

⁴ Patent Owner also maintained in the ’237 IPR that “[t]he *Decision’s* construction addresses a common aspect of a conventional DNS and the disclosed embodiments, namely that a request to look up an address of one entity may be received at another entity. However, the construction overlooks the aspects distinguishing the ‘intercepting’ phrase from conventional DNS.” ’237 PO Resp. 26 (emphases added) (internal citation omitted).

between receiving and intercepting. According to Petitioner’s proposed construction, an “interception” by (intermediate) proxy DNS includes “receiving” a request to look up an address for another (downstream) entity (i.e., the request pertains to that downstream entity). Furthermore, as quoted above, Patent Owner agreed in the ’237 IPR that Petitioner’s construction captured “the disclosed embodiments.” ’237 PO Resp. 26; *supra* note 4. In essence, Petitioner’s construction captures the notion of interception as disclosed in the ’705 patent, by requiring receiving to “pertain” to another entity.

Patent Owner alleges that Dr. Tamassia adopted an “intended for” requirement in the “interception” clause. PO Resp. 33–34 & n.3. Patent Owner points to a portion of the ’237 IPR institution decision outlining a discussion by Dr. Tamassia. *See id.* at 33 (citing Ex. 1005 ¶ 122) n.3 (citing ’237 IPR, Paper 15, 12). Petitioner disagrees with any intent requirement, and contends that Patent Owner mischaracterizes Dr. Tamassia’s testimony. *See* Pet. Reply 14–15.

Patent Owner only addresses this “intent” requirement in an attempt to distinguish its claims over the prior art, and does not propose it as part of its claim construction. *See* PO Resp. 33–34. Furthermore, any alleged prior requirement of “intent” did not survive to the ’237 FWD. *Compare* ’237 IPR, Paper 15 (institution decision), 13, *with* ’237 FWD 10–12. More importantly, Patent Owner does not allege or attempt to show that the ’705

patent supports or requires such “intent” as part of the broadest reasonable construction of the interception term. The record does not support it.⁵

Based on the foregoing discussion, the record shows that the additional functionality urged by Patent Owner should not be imported into the intercepting phrase and Petitioner’s construction tracks the claim and Specification. Accordingly, consistent with the ’237 FWD, the broadest reasonable construction of the term “interception of a request” is “receiving a request pertaining to a first entity at another entity.”

2. Determination, in Response to the Request, Whether the Second Network Device is Available for Communication

In the ’237 FWD, we interpreted the related phrase, “determining, in response to the request, whether the second network device is available for secure communication,” to mean “determining[, in response to the request,] if the second network device is accessible for use, at hand, or usable in a system that provides secure communication using that device.” ’237 FWD 15.

In the ’237 IPR, Patent Owner agreed that focusing on the requester’s security level, and by implication, the relative security levels of the requester and the device, is not required: The “‘determining’ phrase *need not be limited* to the Decision’s determining ‘permission level or security privileges of the requester.’” ’237 FWD 14 (emphasis by Board supplied in the ’237 IPR) (quoting ’237 PO Resp. 29).

⁵ Although not part of the claim construction, a requestor may “intend” for the entered domain name in a request to reach the target device, but the DNS intercepts it to perform the look-up.

The Specification supports this interpretation:

If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site.

Ex. 1050, 40:8–13.

The first quoted sentence in the passage indicates that determining whether a device is “available for a secure communication service” is broad enough to mean determining whether the device is listed on a network database that a secure network uses to obtain access to secure target devices. Therefore, the quoted passage from the Specification, bolstered by Patent Owner’s arguments, indicates that determining if a secure device is listed in an “internal table” (or similar database/DNS structure) of secure sites is sufficient to constitute a determination of availability.

As part of the disclosed process, the system returns a “resolved address” for the target device: “The address that is returned need not be the actual address of the destination computer.” *Id.* at 40:24–25. Furthermore, the determination does not require an actual look-up and resolution into an IP address to occur. *See, e.g.,* Ex. 1001, 40:6–35 (returning a “host unknown” without necessarily looking up an IP address “if a user had requested lookup of a secure web site but lacked credentials”).

Another passage describes a normal DNS “look-up function”:

For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently “passes through” the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

Id. at 39:56–63.

In summary, according to disclosed embodiments in the '705 patent Specification, a device may be determined to be available as a secure device that the system provides, for example, by determining that the device is listed for use as part of the secure system. According to one of the above disclosed examples, which is not limiting, different users may be denied or granted access depending on that particular user's security privileges relative to the target's security level, rendering that device available or unavailable to that user.

Based on the foregoing discussion, according to the '705 patent Specification and the arguments presented, “determination, in response to the request, whether a second network device is available for secure communication,” means “determination, in response to the request, if the second network device is accessible for use, at hand, or usable, in a system that provides secure communication using that device.”

3. Secure Domain Name

Claims 7 and 22 depend respectively from claims 1 and 16, and further specify that the domain name is a “secure domain name.” Relying, in part, on a related *inter partes* proceeding, Petitioner argues “secure domain name” is “a name that corresponds to a secure computer network address.” Pet. 15 (citing '481 institution decision, 8; Ex. 1005 ¶ 141) (emphasis omitted); *accord* '481 FWD 14–14 (same claim construction).⁶

⁶ As indicated above, we refer to *Apple Inc. v. Virnetx, Inc.*, IPR2014-00481 (“'481 IPR”), slip. op. at 8 (PTAB Sept. 3, 2014) (Paper 11) (“'481 institution decision”); *see also* '481 IPR, slip op. at 13–14 (PTAB Aug. 24, 2015) (Paper 35) (“'481 final written decision” or “'481 FWD”).

Petitioner contends its proposed construction is consistent with the Specification. *See* Pet. 15 (citing Ex. 1050, 51:15–51 (arguing the disclosure “describes a ‘secure domain name’ as a domain name that corresponds to the secure network address of a secure server 3320”)). Petitioner relies on additional Specification disclosure in support of its construction. *Id.* (citing Ex. 1050, 40:6–13).

Patent Owner acknowledges that the Board adopted Petitioner’s proposed construction in the ’481 IPR. PO Resp. 22. However, Patent Owner contends that “secure domain name” means “[a] non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS).” *Id.* (Table). Patent Owner argues multiple parties agreed upon its proposed construction in a related district court case. *Id.* (citing Ex. 2015, 19–20) (*Virnetx Inc. v. Apple Inc.*, Case 6:10-cv-00417-LED (E.D. Tex., Dec. 21, 2011) (Joint Claim Construction Chart)). Patent Owner also cites to the Specification as further supporting its proposal and showing that the “secure domain name” is a “nonstandard domain name.” *Id.* (citing Ex. 1050, 7:29–31, 39–42, 50:31–46, 51:15–19, Figs. 33–34; 2018 ¶¶ 36–38). Patent Owner also cites the Monroe Declaration. *Id.* (citing Ex. 2018 ¶¶ 36–38).⁷ Dr. Monroe contends, *inter alia* (see note 7), that the ’705 patent discloses that “[t]o obtain the URL for a ‘secure domain name,’ ‘a secure domain name service (SDNS)’ must be queried.” Ex. 2018 ¶ 37 (citing Ex. 1050, 50:44–46; Figs. 33, 34).

⁷ The cited portion of the Monroe Declaration lists examples in the ’705 patent and prosecution history statements from a related patent as support for Patent Owner’s construction and mirrors Patent Owner’s arguments.

Patent Owner further contends it disclaimed Petitioner's proposed construction in a now completed *inter partes* reexamination of a related patent. PO Resp. 24 (citing Ex. 2016 (Control No. 95/001,270, U.S. Pat. No. 7,188,180, Response to Office Action, Apr. 19, 2010), 5; Ex. 2017 (Right of Appeal Notice, Dec. 3, 2010), 4). Patent Owner stresses that claim construction requires consultation of the prosecution history. *Id.* at 14–15 (citing *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015); *Straight Path IP Grp., Inc. v. Sipnet EU S.R.O.*, 806 F.3d 1356, 1362 (Fed. Cir. 2015)). Patent Owner also appears to acknowledge that prosecution history disclaimers do not bind the PTO. *See id.* at 11 (citing *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 978 (Fed. Cir. 2014) (The “court also observes that the PTO is under no obligation to accept a claim construction proffered as a prosecution history disclaimer, which generally only binds the patent owner.”)).

Beginning with the claim language, dependent claims 7 and 22 recite that the domain name is a “secure domain name.” Petitioner's proposed construction involves the plain meaning of those words, “a name that corresponds to a *secure* computer network address.” Any construction under the broadest reasonable standard should not obscure the clarity of the claim language. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (en banc) (“In some cases, the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words.”). The Specification may set out a particular meaning of a claim term that diverges from its plain meaning so long as it does so “with

reasonable clarity, deliberateness, and precision.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). “Without an express intent to impart a novel meaning to claim terms, an inventor’s claim terms take on their ordinary meaning.” *York Prods., Inc. v. Central Tractor Farm & Family Ctr.*, 99 F.3d 1568, 1572 (Fed. Cir. 1996).

The ’705 patent describes as an “example,” replacing a standard top-level domain name like .com, with “a[n] s.com top-level domain name, where the ‘s’ stands for secure.” Ex. 1050, 50:35–38. It describes top-level domain alternatives: “Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name.” *Id.* at 50:38–40. The ’705 patent also states that “[b]ecause the secure *top-level domain name* is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown.” *Id.* at 50:41–44 (emphasis added).

This latter disclosure about what a standard DNS may or may not return applies to the examples of non-standard *top-level* domain names, but Patent Owner does not urge a non-standard *top-level* domain name in its construction. The Specification also does not imply or expressly state that all of the disclosed “secure domain names” must include a “top-level” domain name, and it implies in other places that secure DNSs can resolve secure domain names using internal tables or similar databases—in other words, using a conventional look-up process. For example, the Specification states that “SDNS 3313 contains a cross-reference data base of secure domain names and corresponding secure network addresses. That is, for

each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name.” *Id.* at 51:15–18.

As Petitioner contends, this disclosure, and others, imply that a “secure domain name” is a domain name that “corresponds to the secure network address” for a secure device. *See* Pet. 15 (citing Ex. 1050, 51:6–42). Other disclosures support Petitioner’s broader construction: “An entity can register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website.” *Id.* at 51:19–22. An entity can register “several secure domain names” representing a “hierarchy of access,” and “different priority level of access,” with fees varying for “a desired level of guarantee” for secure access. *Id.* at 51:22–32. Furthermore, in addition to resolving names based on the name itself, “SDNS 3313 determines the particular secure computer network address based on the user’s identity and the user’s subscription level.” *Id.* at 51:34–37.

Therefore, based on the above-cited disclosures, although some of the disclosed examples that Patent Owner relies upon show that a conventional DNS does not return a secure address if it has a non-standard *top-level* domain name (e.g., .scom), the Specification in its entirety does not support the construction that requires a conventional DNS, or a secure DNS using a conventional process, not to return the secure domain names contemplated by the invention. The last few disclosures listed in the previous paragraph and others indicate that the security address returned does not depend solely on the type of secure domain name—it also depends at least partly on the user’s identity and/or subscription level. This implies further that a secure

domain name need not be non-standard, because the resolution of it depends on other “non-standard” factors like the user’s identity or security level. Similarly, rather than a conventional domain name service not returning a secure address based solely on the name, the Specification states that a “DNS *proxy*” returns a “host-unknown” “if the user had requested look[-]up of a *secure web site but lacked credentials to create such a connection.*” *Id.* at 40:30–33 (emphases added). “In this manner, different users requesting access to the *same [secure] DNS name* could be provided with different look-up results.” *Id.* at 40:33–35 (emphasis added).

According to the passage quoted above in previous Section I.D.2, requests for *non-secure* websites are “passe[d] through” to provide a “normal look-up function,” “provided that the requesting host has permissions to resolve unsecured sites” (again, so that “[d]ifferent users who make identical DNS requests get different results”). Ex. 1050, 39:58–63. This latter disclosure, describing a “normal look-up function,” for non-secure websites, does not imply or dictate that a request for secure access requires an unconventional DNS look-up function. Rather, as noted at the outset (Section I.A), and by way of example, the ’705 patent describes “the automatic creation of a virtual private network (VPN) *in response to a domain-name server look-up function.*” Ex. 1050, 39:4–6 (emphasis added). In one embodiment, “[a] specialized DNS server traps DNS requests” from users “for which secure communications are defined” and may return “different results” to an “identical DNS request” for setting up a VPN, *id.* at 1050, 39:46–49, 61–62. Eventually, a DNS proxy returns a “resolved address” (passed by a gatekeeper) that may or may not be the “actual address.” *Id.* at 40:21–25. In any case, a DNS proxy “determines “[i]f

access to a secure site has been requested . . . by a domain name extension *or by reference to an internal table of such sites.*” *Id.* at 40:10–11.

In addition to determining if a secure domain name has been requested “by reference to an internal table” (*id.*), the Specification combines conventional and proxy DNS functions—“combining the functions of the two servers” to form a “single server.” Ex. 1050, 40:47. Hence, the Specification contemplates using conventional DNS look-up functions for secure domain names by combining that functionality with different proxy DNS functions. According to a passage in the ’705 patent and testimony by Dr. Tamassia, a conventional DNS looks up an address for a name. *See* Ex. 1050, 50:39:7–10; Ex. 1005 ¶¶ 150, 164–66 (“much like a file system”), 341–44 (describing well-known DNS functionality as disclosed in Beser and the ’705 patent as providing a look-up function); *infra* note 17 (evidencing DNS functions).

Furthermore, in one of Patent Owner’s related ancestor patents, U.S. Pat. No. 6,502,135, claim 1 requires “determining whether the *DNS request* transmitted in step (1) is requesting access to *a secure web site.*” (Emphasis added). This patent claim does not preclude a “non-conventional” DNS from resolving the access request for a secure web site. *See, e.g., Mangrove Partners Master Fund, Ltd., v. Virnetx Inc.*, IPR2015-01046, slip op. at 6–7 (PTAB Sept. 9, 2016) (Paper 71) (noting that Patent Owner characterized the DNS request or resolution in claim 1, in response to a question at oral argument, as something that could be “conventional - - non-conventional or whatever”).

Therefore, Patent Owner’s construction and its prosecution history arguments (as discussed further below) obscure the clear meaning of the

claim term—because they attempt to preclude the ability of a “conventional” DNS from resolving a “non-standard” name. As the record shows, the conventional DNS functionality at issue simply involves looking up names (using for an example an internal table or similar structure). Therefore, if a DNS resolves a non-standard name (whatever that means especially if not limited to a top-level domain name), the resolution itself would be “conventional,” whereas Patent Owner’s construction implies that any DNS that resolves a “non-standard” name cannot be “conventional.”

As indicated above, Federal Circuit precedent indicates that prosecution history must be consulted in claim interpretation, but it does not necessarily bind the PTO. *See Philips*, 415 F.3d at 1317 (“[T]he prosecution history provides evidence of how the PTO and the inventor understood the patent. . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes.”); *Tempo Lighting*, 742 F.3d at 978 (The “court also observes that the PTO is under no obligation to accept a claim construction proffered as a prosecution history disclaimer, which generally only binds the patent owner.”).

In this case, the Specification and plain meaning of the claims do not support the prosecution history arguments and those arguments obscure the plain meaning. *See Phillips*, 415 F.3d at 1316 (“The construction that stays true to the claim language and most naturally aligns with the patent’s description of the invention will be, in the end, the correct construction.” (citation omitted)). Attempting to support its claim construction arguments discussed above, Patent Owner contends that it disclaimed “a domain name

that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization” during an *inter partes* reexamination of a related patent, and that the Specification supports its construction. PO Resp. 23 (citing Ex. 2016, 5; 2017, 4). Patent Owner explains that its argument about what a “secure domain name just happens to be associated with” means that “a secure domain name cannot be resolved by a conventional domain name service.” *Id.* (citing Ex. 2017, 4); *accord* Ex. 2016, 6 (arguing “a secure domain name cannot be resolved by a conventional domain name service, for example,” relying on “the inventors . . . acting as their *own lexicographers*,” and citing disclosed examples in the ’180 patent of non-standard top-level domain names) (emphasis added).

But as explained above, this argument presents unclear distinctions that obscure the meaning of the challenged claims when viewed in light of the Specification’s disclosure of secure domain names. Contrary to the prosecution history arguments, nothing in the ’705 (or ’180) patent precludes conventional DNS functionality from resolving disclosed secure domain names, let alone, sets forth a *lexicographic* definition for such a preclusion. Rather, as noted above, the ’705 patent discloses using conventional DNS look-up functionality (*e.g.*, using internal tables) to determine whether access to a secure website has been requested, adding other layers of functionality, including employing user priority levels, and/or credentials, etc. *See, e.g.*, Ex. 1050, 40:6–13 (“proxy . . . intercepts all DNS look[-]up functions” and determines access “by reference to an internal table”), 44–48 (combining proxy and conventional “functions . . . into a single server”), 57–67 (using “an internally stored list of authorized IP addresses”), 51:22–36 (users can “automatically obtain the secure computer network address” by

“register[ing] a secure domain name” with possible additional use of “the user’s identity and the user’s subscription level”); note 5 (describing “a common aspect of *a conventional DNS and the disclosed embodiments*”).⁸

Patentee’s stated attempt during prosecution of the ’180 patent to act as its “own lexicographer[]” by relying on *examples* in the ’180 patent that relate to non-standard *top-level* domain names that something must look up to resolve (Ex. 2016, 6; *see also supra* note 8) obscures clarity and fails to support the prosecution history disclaimer argument. Contrary to Patentee’s assertion of a lexicographic definition during prosecution, no reasonably clear and precise disclaimer appears in the Specification with respect to secure domain names. *See, e.g., Paulsen*, 30 F.3d at 1480 (disclaimer requires “reasonable clarity, deliberateness, and precision”).

And Patent Owner does not argue here that the ’705 patent supports a lexicographic definition for a secure domain name. Examples related to top-level domain names in the Specification cannot support an alleged

⁸ The Examiner’s citations and reasoning in the 95/001,270 reexamination proceeding involving the ’180 patent track Patent Owner’s arguments and do not support the specific disclaimer argued. The Examiner states that “[f]or example, the ’180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name.” Ex. 2017, 6 (citing ’180 patent, 51:25–53). Citing the same passage, the Examiner also states that “querying a convention[al] domain name server using a secure domain name will result in a return message indicating that the URL is unknown.” *Id.* at 7. As explained above, these cited examples do not support a clear disclaimer that distinguishes a “secure domain name,” because, for example, the cited ’180 patent disclosures describe examples that correspond to a non-standard *top-level* domain name. *See* ’180 patent, 51:25–53. As explained herein, the ’705 patent does not preclude conventional DNS look-up functionality for all secure domain names.

lexicographic definition for all the secure domain names (especially when Patent Owner does not limit its construction to top-level domain names). *See id.* Moreover, Petitioner points out that Patentee argued during prosecution of a related patent that the term “secure name” encompasses a “secure non-standard domain name” such as “a secure nonstandard top-level domain name (*e.g.*, .scom) or a **telephone number**.” Pet. Reply 17 (citing Ex. 1069, 9). The prosecution history cited by Petitioner shows that Patentee urged a construction that more closely tracks Petitioner’s construction here and does not require a conventional DNS not to recognize a non-standard name (and does not require a non-standard name):

*Applicant submits that a “secure name” is a name associated with a network address of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device. The claimed “secure name” includes, but is not limited to, a secure domain name. For example, a “secure name” can be a secure non-standard domain name, such as a secure non-standard top-level domain name (*e.g.*, .scom) or a telephone number.*

Ex. 1069, 9 (emphases added).

Similarly, in addition to the just-described prosecution history, in the final written decision in the ’481 IPR, the Board found that “Patent Owner . . . made the opposite argument to a district court that it is making here, and argued that the ‘non-standard’ distinction ‘is not supported by the specification or the prosecution history.’” ’481 FWD, 13 (quoting ’481 Ex. 1018, 18 (district court findings and rationale)).⁹ The record here supports

⁹ The district court case cited in the ’481 IPR construed a different term: “secure domain name service.” *See* ’481 Ex. 1018, 17–18. The Board

the argument made by Patent Owner in the district court—i.e., the Specification and prosecution history do not support the “non-standard” distinction. Given Patent Owner’s various arguments in different proceedings, our finding that the Specification does not support a lexicographic definition for secure domain names, and the lack of clarity carried by the proposed construction, the record does not support Patent Owner’s assertions of prosecution history disclaimer. Petitioner’s construction constitutes the broadest reasonable construction because it tracks more closely to a “secure domain name” as described in the Specification.

Based on the foregoing discussion, a “secure domain name” is “a name that corresponds to a secure computer network address.”

II. OBVIOUSNESS ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner’s expert, Dr. Tamassia, states that a person of ordinary skill in the art would have “a good working knowledge of networking protocols, including those employing security techniques, as well as cryptographic methods and computer systems that support these protocols and techniques.” Ex. 1005 ¶ 148; *see* Pet. 8. Such a person would have gained this

construed a “secure domain name service” in the ’481 IPR as “[a] service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service [(“DNS”)] cannot resolve addresses.” ’481 FWD 14–25 (adopting petitioner’s construction in that case). The functionality described with respect to the conventional DNS need not carry into the secure domain name itself. *See* ’481 FWD 13–14 (construing “secure domain name” as “a name that corresponds to a secure computer network address”).

knowledge “either through several years of practical working experience or through education and training” or some combination of both. *Id.*

Patent Owner argues that “[a]person of ordinary skill in the art at the relevant time would have had a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security.” PO Resp. 2 n.1 (citing Ex. 2018 ¶¶ 13–14). Dr. Monroe states that “a person of ordinary skill in the art [at the relevant time] would have had a master’s degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security.” Ex. 2018 ¶ 13.

Patent Owner’s description of the background of a person of ordinary skill in the art is not inconsistent with Petitioner’s description. Instead, Patent Owner’s definition requires a particular educational background, but appears to result in the same level of expertise as Petitioner’s definition. For purposes of this Decision, based on the testimony of the parties’ experts as well as our review of the ’705 patent and the prior art involved in this proceeding, we conclude that a person of ordinary skill in the art would have a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security—or the equivalent, obtained through practical work experience and training.

*B. Tamassia Declaration*¹⁰

Patent Owner argues that the entirety of the Tamassia Declaration should be given little or no weight because Dr. Tamassia “failed to consider, let alone opine on, how any of the claim features are disclosed in asserted references.” PO Resp. 47. Petitioner responds that Dr. Tamassia has “offered probative testimony on many of the factual inquiries underpinning an obvious analysis” that “can certainly ‘assist the tier of fact to understand the evidence or determine a fact in issue.’” Pet. Reply 23 (citing Fed. R. Evid. 702). Petitioner adds that “no rule requires an expert to opine on the ultimate question of obviousness or on every potentially relevant fact at issue for his opinion to be admissible or entitled to weight.” *Id.* at 23–24.

Patent Owner has not articulated a persuasive reason for giving Dr. Tamassia’s declaration, as a whole, little or no weight in our analysis. We agree with Petitioner that experts are not required to opine on every relevant factual and legal issue in order to be accorded substantial weight. The cases Patent Owner relies on do not persuade us otherwise. For example, Patent Owner cites *Schumer v. Laboratory Computer Systems, Inc.*, 308 F.3d 1304, 1315 (Fed. Cir. 2002), for the proposition that “expert testimony ‘must identify each claim element, state the witnesses’ interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference.’” PO Resp. 48–49. Patent Owner’s quotation, however, mischaracterizes *Schumer* by omitting introductory words necessary to the meaning of the quoted sentence. In its entirety, the quoted portion of *Schumer* states the following:

¹⁰ We address Patent Owner’s Motion to Exclude (Paper 30) certain paragraphs of Exhibit 1005 in a separate section, below.

Typically, testimony concerning anticipation must be testimony from one skilled in the art and must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference. The testimony is insufficient if it is merely conclusory.

Schumer, 308 F.3d at 1315–16. The Federal Circuit then adds that it is not the task of the courts to “attempt to interpret confusing or general testimony to determine whether a case of invalidity has been made out” and “if the testimony relates to prior invention and is from an interested party, as here, it must be corroborated.” *Id.* at 1316. So, instead of laying out a specific, required format for the content of all testimony regarding invalidity, as asserted by Patent Owner, this portion of *Schumer* confirms the unremarkable proposition that conclusory, overly general, confusing, and self-interested testimony should not be relied upon. *Id.*; *see also Koito Mfg. v. Turn-Key-Tech, LLC*, 381 F.3d 1142, 1152 (Fed. Cir. 2004) (“General and conclusory testimony, such as that provided by Dr. Kazmer in this case, does not suffice as substantial evidence of invalidity.”). Patent Owner has not shown that the whole of Dr. Tamassia’s testimony suffers from any of these failings.

Under 37 C.F.R. § 42.1(d), we apply the preponderance of the evidence standard in determining whether Petitioner has established unpatentability. In doing so, it is within our discretion to determine the appropriate weight to be accorded the evidence presented, including expert opinion, based on the disclosure of the underlying facts or data upon which that opinion is based. Thus, we decline to make a determination about Dr. Tamassia’s opinion, as a whole. Rather, in our analysis we will consider, as

it arises, relevant portions of Dr. Tamassia's testimony and determine the appropriate weight to accord that particular testimony.

C. Prior Art Printed Publication Status of RFC 2401

Patent Owner asserts that Petitioner has not sufficiently established that RFC 2401 qualifies as a printed publication as of its alleged publication date. PO Resp. 51–59. The determination of whether a document is a “printed publication” under 35 U.S.C. § 102(b) involves a case-by-case inquiry into the facts and circumstances surrounding its disclosure to members of the public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004); *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1364 (Fed. Cir. 2014). Public accessibility is a key question in determining whether a document is a printed publication and is determined on a case-by-case basis. *Suffolk Techs.*, 752 F.3d at 1364. To qualify as a printed publication, a document “must have been sufficiently accessible to the public interested in the art.” *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009) (citation omitted).

In our Decision to Institute, we found that RFC 2401 includes indicia suggesting a reasonable likelihood that the document was made public and accessible because (1) RFC 2401 is a dated “Request for Comments” from the “Network Working Group,” discussing a particular standardized security protocol for the Internet, and (2) it 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.” Inst. Dec. 6–7 (citing Ex 1008, 1). On this basis, we determined that Petitioner had met its burden for a threshold showing to proceed to trial. *Id.*

In support of Petitioner’s position, 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. 1005 ¶ 186. Dr. Tamassia also relies on an RFC publication that discusses the RFC development and publication process itself—RFC 2026, dated October 1996. *Id.* ¶¶ 187–193 (citing Ex. 1036). 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.* at ¶ 190. 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. 1005 ¶ 189 (quoting Ex. 1036, 8). Each RFC “is published as part of the ‘Request for Comments’ (RFC) document series RFCs can be obtained from a number of Internet hosts using . . . World Wide Web, and other Internet document retrieval systems.” *Id.* ¶ 187 (quoting Ex. 1036, 6).

Patent Owner argues that Petitioner cannot rely on evidence it has proffered to support this finding. First, Patent Owner argues that testimony by Dr. Tamassia should not be accorded any weight because Dr. Tamassia has not been established to have personal knowledge that RFC 2401 was actually released to the public in November 1998 nor has Dr. Tamassia “been established as someone familiar with, let alone an expert in, the

workings of the internet Engineering Task Force (IETF)—the body responsible for the RFCs.” PO Resp. 54.¹¹

We find 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 which Patent Owner does not challenge.¹² As part of routine discovery, *see* 37 C.F.R. § 42.51(b)(1)(ii), Patent Owner had the opportunity to cross-examine Dr. Tamassia, but does not point us to any discussion of this issue. Moreover, RFC 2401’s contents are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including the inclusion of a date “November 1998” on the top right corner of the first page of the document. Ex. 1008, 1. In addition, this document—a request for suggestions and improvements for an Internet standards protocol, having no indication of being a mere draft or internal paper—is precisely the type of document whose very purpose is public disclosure, including on the Internet.

“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*

¹¹ Patent Owner also argues we should give Dr. Tamassia’s testimony on this issue no weight because the Petition does not cite to these paragraphs. PO Resp. 54 n.5. Patent Owner, itself, however, directed the Board’s attention to this testimony in its Preliminary Response (Paper 6, 3–4), and, thus, clearly has had adequate notice of its contents such that it may respond with no resulting prejudice.

¹² As addressed below, Patent Owner objects and moves to dismiss a number of Exhibits based on hearsay and relevancy without addressing any one in particular, including Exhibit 1036.

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)). We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401 (dated November 1998) was disseminated and made available to persons of ordinary skill interested in computer networking and security to be deemed “publicly accessible” at the relevant time. Therefore, on this record, we determine RFC 2401 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

D. Beser

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:

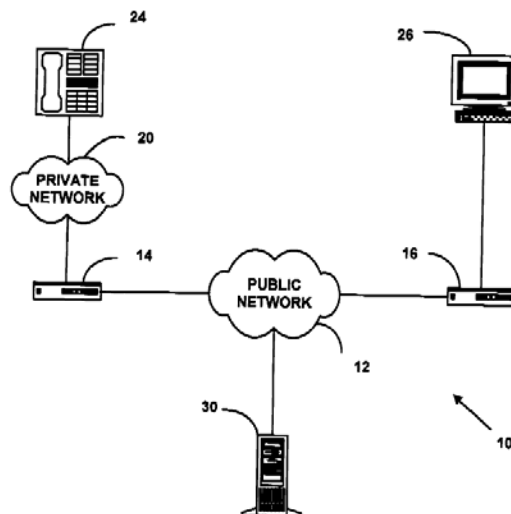


Figure 1 of Beser’s system depicts public network 12 (for example the Internet), network end devices 24 and 26 on private networks 20, trusted-

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 networks 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, 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, 5.¹³ 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 ends of the VoIP [(Voice-over- Internet-Protocol)] association by methods known to those skilled in the art.” *Id.* at 12:33–37.

¹³ 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.

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.

E. RFC 2401

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.*

F. Representative Claims

As indicated above, Petitioner asserts that the combination of Beser and RFC 2401 would have rendered claims 1–23 and 25–30 obvious, and that the combination of Beser, RFC 2401, and Brand would have rendered claim 24 obvious. Patent Owner presents separate patentability arguments for claims 1, 6, 7, and 13, with parallel arguments for claims 16, 21, 22, and 28. *See* PO Resp. 42–46. Patent Owner asserts that remaining challenged claims 2–5, 8–12, 14, 15, 17–20, 23–27, 29, and 30 are patentable because they depend from claims 1 or 16. PO Resp. 47. Accordingly, this Final Written Decision focuses on claims 1, 6, 7, and 13 as representative of the challenged claims. *See* Paper 9, 3 (“[P]atent [O]wner is cautioned that any arguments for patentability not raised in the [R]esponse will be deemed waived.”). In addition, because Petitioner bears the burden of persuasion to show unpatentability on all the challenged claims, we address the record to consider the challenges.

G. Obviousness Challenge

Petitioner asserts that Beser’s “non-encrypted streaming audio/video example” and other showings (*see* Pet. 28 & n.3) encompass almost all of the limitations of claims 1 and 16, but Petitioner proceeds on an assumption that Beser does not disclose explicitly all elements of the recited determining step and the related “secure communications link,” under a claim construction that assumes that the claimed link requires encryption for data traffic on the link. *See id.* at 28–29, 34–42. Specifically, Petitioner argues that the claim 1 “client device” reads on Beser’s originating end device 24, and that the claim 1 “target device” reads on Beser’s terminating end device 26. *See id.* at 34–35.

Petitioner explains that Beser's trusted-third-party network device 30 negotiates private IP addresses with first 14 and second 16 network devices based on a request that includes a unique domain name for the claimed "target device" *See id.* at 34–37. For example, according to Petitioner, Beser's "trusted-third-party network device [30] . . . with the help of the first [14] and second [16] network devices, establishes a private tunneling association" by processing requests for access to a WebTV source or for initiating a VoIP call. *Id.* at 34–35 (citing Ex. 1007, 4:43–54, 7:64–66, 15–20, 10:22–36, 10:55–66, 14:51–67; Ex. 1005 ¶¶ 316, 354, 358, 362, 373–78, 383).

Petitioner contends that Beser's negotiating devices (14, 30, and 16, *see* Ex. 1007, Fig. 9), as modified by RFC 2401, thereby facilitate a connection with terminating end device 26 over a secure network created in response to interception of a request to look up an internet address based on a domain name for end device 26, and determines as a result that end device 26 is a device with which a secure communication link can be established, as claim 1 requires. *See id.* at 34–39, 45–46 (asserting interception by first network device 14 and trusted-third-party device 30); Ex. 1007, Figs. 1, 4, 5. According further to Petitioner, it would have been obvious to a person of ordinary skill in the art to provide "end-to-end" encryption of the traffic being sent to Beser's end device 26 using the teachings of RFC 2401. *See* Pet. 29–30. Petitioner explains that it would have been obvious to determine whether a secure link can be established using a trusted third-party device 30 as a DNS server, and "encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses to establish a private IP tunnel."

Pet. 45 (citing Ex. 1007 4:9–11, 9:6–11, 9:26–30, 11:9–58; Ex. 1005 ¶¶ 314–15, 345–46, 361, 368, 371, 373–78). Petitioner summarizes with respect to the determination step based on the combination: “Because in this configuration all IP tunnels would have been encrypted, the determination that the terminating device can establish an IP tunnel is a determination that it accepts encrypted communications (*“that a secure communication link can be established”*).” Pet. 39–40 (citing Ex. 1007, 1:54–56, 11:26–58; Ex. 1005 ¶¶ 361–63, 368, 431, 433, 436–37).

Petitioner contends that “[i]n any scenario, if the unique identifier [domain name] is not registered, the trusted-third-party network device would not negotiate an IP tunnel.” *Id.* at 39 (citing Ex. 1005 ¶ 363). As a consequence, “Beser shows a ‘determination’ as specified in claims 1 and 16.” *Id.* (emphasis omitted). Petitioner argues that the combination of Beser and RFC 2401 would have rendered obvious the determination step “[b]ecause in this [modified] configuration all IP tunnels would have been encrypted, [such that] the determination that the terminating device can establish an IP tunnel is a determination that it accepts encrypted communications (*“that a secure communication link can be established”*).” *Id.* at 39 (citing Ex. 1007, 1:54–56, 11:26–58; Ex. 1005 ¶¶ 361–63, 368, 431, 433, 436–37).

Petitioner also contends that the combination of Beser and RFC 2401 teaches or suggests the remaining elements of claims 1 and 16, including the recited memory, application for “allow[ing] participation in audio/video communications over the secure communication link,” and processing configuration for the application. *See id.* at 40–42 (Ex. 1007, 4:43–54, 5:15–47, 6:24–57, 8:15–18, 9:64–10:2; Ex. 1005 ¶¶ 326–27, 331, 350).

Petitioner articulates several reasons, supported by the record, for combining the two references. For example, “several passages of Beser plainly indicate that encryption should be used and criticize prior art techniques that prevent use of end-to-end encryption.” Pet. 32 (citing Ex. 1007, 2:22–27, 11:22–25, 18:2–5, 20:11–14). Petitioner also contends that RFC 2401 and Beser “show[] precisely the same network topology,” with RFC 2401 disclosing and suggesting “end-to-end encryption” in its “IPsec case 3 design” to “hid[e] the data,” thereby enhancing Beser’s “IP tunnel [that] provide[s] anonymity over the public network, hiding the true source and destination addresses.” Pet. 31–32 (citing Ex. 1007, 1:54–56, 4:7–8, 4:18–29, Fig. 1; Ex. 1005 ¶¶ 427–28, 431–32, 434–38; Ex. 1008, 25). In other words, Petitioner shows persuasively that it would have been obvious in view of the teachings in Beser and RFC2401 to provide end-to-end encryption in order to enhance security. The record supports Petitioner’s showing, and we adopt that showing, as summarized above, as our own.

1. Interception of a Request

Shown in context to the preamble and its preceding clause, the “interception” clause of claim 1 follows:

1. A client device comprising (a) memory configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on
 - (i) *interception of a request*, generated by the client device, to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device.

Ex. 1050, 55:53–58 (emphasis added).

Claim 16 recites a similar element. *Id.* at 56:39–46. As construed above, the term “intercepting a request” means “receiving a request pertaining to a first entity at another entity.” Section I.D.1. As indicated

above, Petitioner contends that the tunneling request in *Beser* “is actually ‘intercepted’ by each of the first network device and the trusted-third-party network device because they each ‘receive’ a request pertaining to a first entity at another entity.” Pet. 46. Petitioner explains that in *Beser*’s system, “the request contains a unique identifier associated with the terminating end device.” *Id.* (citing 8:21–47, 22:8–22; Ex. 1005 ¶¶ 124, 355, 360). In other words, because the tunneling request includes a unique identifier associated with terminating end device 26, Petitioner contends that it “pertains to” the terminating end device, and is received (intercepted) by another entity—first network device 14 and/or trusted-third-party network device 30. *See id.* (citing Ex. 1007, 8:21–47; 22:8–22; Ex. 1005 ¶¶ 124, 355, 360).

Patent Owner responds that the tunneling request cannot be “intercepted” by first network device 14 or trusted-third-party network device 30, because in *Beser*’s system, “requests always go to, and are always intended to go to,” first network device 14 and trusted-third-party device 30. *See* PO Resp. 35 (citing Ex. 2018 ¶ 53). Patent Owner contends that Petitioner’s expert, Dr. Tamassia, adopted this “intended for” requirement as an interpretation of “interception,” and *Beser* does not satisfy the requirement. *Id.* at 33–34 (citing Ex. 2018 ¶ 51; Ex. 2019, 80:3–13).

Patent Owner’s contentions are not persuasive. As set forth above, the “interception” clause does not require any intent. Section I.D.1 (Claim Construction). Furthermore, as Petitioner argues, no party proposed an “intent” element as part of its proposed claim construction of the

“interception” clause in this proceeding. See Pet. Reply 14; PO Resp. 4 (listing both parties’ claim construction proposals).¹⁴

In any event, as Petitioner explains, regardless of what this “intent” requirement entails, in Patent Owner’s disclosed system, all requests are intended to go to the proxy DNS (i.e., not another entity), which the Specification characterizes as “intercept[ing] all look[-]up functions” (Ex. 1050, 4:6–7):

The ’0705 patent’s only disclosure of a DNS device that “intercepts” lookup requests is DNS proxy 2610, which “intercepts ***all DNS lookup functions*** from client 2605.” Ex. 1050 at 40:6–7 (emphasis added). The ’0705 patent thus provides that DNS proxy 2610 “intercepts” lookup functions, even though the DNS proxy receives every single lookup request sent by the client. *Id.* at Fig. 26, 40:6–7. Dr. Monroe agreed the DNS proxy receives every DNS request and that the system is designed, *i.e.*, “pre-established” to intercept every DNS request. Ex. 1066 at 55:8–20. Thus, the Board should reject Patent Owner’s arguments that Beser cannot show “intercepting” because it is designed such that IP tunnel requests are received by network device 14 and trusted device 30.

Pet. Reply 13 (emphasis by Petitioner).

As Petitioner argues in the above passage, Dr. Monroe agreed (during his deposition) to Petitioner’s characterization that the ’705 patent’s disclosed proxy DNS intercepts all DNS look[-]up functions. *Id.* (citing Ex. 1066, 55:8–20); Ex. 1066, 55:12–15 (“the DNS proxy does - - it says in that embodiment the DNS proxy intercepts all DNS look[-]up functions from the client”). Therefore, the record shows that Beser’s first network device 14

¹⁴ Accordingly, it is not necessary to reach Petitioner’s explanation that Beser’s originating device 24 “intends for” packets with look-up requests to go to first device 14, and that trusted-third-party device 30 “intercepts” those packets. See Pet. Reply 14.

and trusted-third-party device 30 operate just like the disclosed proxy DNS in the context of intercepting requests. In other words, as explained above in the claim construction section, the '705 patent treats “intercepting” by the intermediate proxy DNS as “receiving” a request to look up an address for another entity (e.g., a target or end device), and both parties agree “receiving” constitutes “intercepting.” Section I.D.1.

2. Request to Lookup an Internet Protocol (IP) Address

Patent Owner also contends that Beser’s tunneling request is not a “request to lookup an internet protocol (IP) address,” as claim 1 recites, because it is “a request to initiate a tunnel.” PO Resp. 31 (citing Ex. 2018 ¶ 47). Patent Owner also argues that Beser’s trusted-third-party device 30 does not negotiate private IP addresses, and that the “negotiation does not involve looking up any IP address, but rather involves *assignment* of a first private network address to the terminating device.” *Id.* at 31–32 (citing Ex. 1007, 12:2–4; Ex. 2018 ¶ 48). Patent Owner also argues that “one of the novel aspects of the claims is that, while a request to look up an IP address is transmitted, the request is intercepted allowing it *not* to be processed in the conventional manner.” PO Resp. 32 (citing Ex. 1050, 40:6–35; Ex. 2018 ¶ 50).

Patent Owner’s arguments are not persuasive. The last argument about what the disclosure “allow[]s” fails to distinguish over Beser and is not clear. The challenged claims do not preclude processing a request in a “conventional” manner to look up an address. *See, e.g., supra* Section I.A, I.D.3 (citations showing look-up functions as part of the disclosed '705 patent invention); *infra* note 4 (Patent Owner arguing that embodiments

include conventional functionality); notes 15–16 (conventional DNS functionality).

The argued “interception of a request . . . to look up an (IP) . . . address” clause in claim 1 does not require actually providing a DNS resolution or a look-up result for the IP address. *See* PO Resp. 32. The “determination as a result of the request” (that a target can be used in a “secure communication link”) clause also does not necessarily require a look-up to resolve an IP address. That clause does not recite a determination as a result of a *look-up*—it recites a “determination as a result of the *request*.” As explained above, the ’705 patent disclosure supports this interpretation and indicates that the breadth of claim 1 includes, as one example, that the result of any request may involve determining if secure communications may be made by using a table of internal target cites (e.g., listing domain names) and then assessing a user’s security level relative to that requested domain name. *See* Ex. 1050, 40:8–13 (internal table), 30–33 (returning a “host unknown” error as opposed to an IP address, “if the user had requested lookup of a secure web site but lacked credentials”); *supra* Section I.D.2.

In any event, to the extent claims 1 and 16 may imply, or read on, a requirement for an actual look-up of an IP address (as part of the determination clause or otherwise), Beser and the ’705 patent each disclose using conventional DNS look-up functionality as a part providing secure communications.¹⁵ *See also* Section I.A, I.D.3

¹⁵ With respect to Beser: “For example, an appropriate Domain Name Server (‘DNS’) inquiry may correlate the IP address with a domain name,

(citations showing look-up functions as part of the disclosed '705 patent invention). The '705 patent's system specifically combines conventional DNS look-up and proxy functions "into a single server." Ex. 1050:45; *see also* note 15. Patent Owner's other arguments create a purported distinction between the claimed "look up" and different "assignments" in Beser that does not exist, because Beser's DNS and/or other data assignment schemes all perform some type of a look-up to resolve a domain name. *See* Pet. Reply 8–12 (persuasively arguing that Beser discloses a "look up" that must be performed to "assign" an address); notes 16–17; *supra* Sections 1.A, I.D.3.

According to Beser, pursuant to the tunneling request, trusted-third-party device 30, with devices 14 and 16, or device 30 by itself, negotiates and looks up a private internet address for end device 26, in part by looking up a public internet address for device 16 based on the domain name associated with end device 26. *See* Ex. 1007, 10:37–57, 11:1–52, 12:6–19, 13:30–33; Pet. Reply 11 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs.6 and 9). The request includes 1) an indicator having "a distinctive sequence of bits" to initiate a secure tunneling action (Ex. 1007, 8:37–38), and 2) "a unique identifier for the terminating end [26] of the tunneling

and domain names are typically descriptive of the user, location, or the user's organization." Ex. 1007, 1:50–53; *see also id.* at 10:55–57 ("Other possibilities are that the unique identifier . . . is a domain name . . . used to initiate the VoIP association."), 10:37–41 (similar). With respect to the '705 patent: "Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host." Ex. 1050, 39:7–9. In addition, according to this conventional scheme, "[w]hen a user enters the name of a destination host, a request DNS REQ is made . . . to look up the IP address associated with the name." *Id.* at 39:17–19.

association” (*id.* at 8:1–3). This unique identifier in a request packet for terminating device 26 may be “a domain name,” or “many other possibilities,” such as an “employee number, social security number, driver’s license number, or even a previously assigned public IP 58 address.” *See id.* at 10:37–41, 10:66–11:2, 11:20–22. Pursuant to the request packets, “[a] public network address for a second network device [16] is associated with the unique identifier on the trusted-third-party network device at Step 106.” *Id.* at 8:4–7. In other words, “the second network device” 16 and its public address are “associated with . . . terminating end [26] of the tunneling association” via the terminating end’s “unique identifier” (a domain name), and/or any number of “database entr[ies],” which provide an association, including “public IP 58 addresses for the terminating . . . device 26.” *See id.* at 8:4–9, 11:45–55. After this association between device 16 and 26, in step 108, “the second private network address is assigned to the terminating end [26] of the tunneling association.” *Id.* at 8:14–15, Fig. 4 (step 108).

The record shows that at least a domain name for terminating device 26 (i.e., “the target device” of claims 1 and 16) in the request packet constitutes a request, intercepted by DNS 30 and device 14, to “look up an internet . . . address of second network device” 26. Beser also discloses actual look-ups, assuming it is required by the determination clause of claim 1 (and a similar clause in claim 16): “determination as a result of the *request* that the target device is a secure communication device with which a secure communication link can be established.”¹⁶ Claim 1 (emphasis added).

¹⁶ In addition to Beser providing a look-up for the private address of device 26, Beser discloses DNS 30 may include a “database entry . . . includ[ing] a public IP 58 address[] *for the terminating telephony device 26*. Many data

In addition to the configuration that includes looking up the public IP address of device 26 by DNS 30 (*see* notes 15, 16), Beser’s network device 16 looks up the private IP address of device 26—after DNS 30 and network device 14 receive the request for a look-up. *See, e.g.*, Ex. 1007, 16:1–37, Fig. 9 (step 156 indicates that second network device 16 “select[s the] second private IP address”); *supra* Section II.D (describing Beser); PO Resp. 33 (describing Beser’s negotiation process to obtain the private address for terminating device 26). Therefore, based on the foregoing discussion and Beser’s disclosure, we find that either of Beser’s devices 14 and/or 30 intercepts a request to look up an internet address of second network device 26, as required by claims 1 and 16.

Patent Owner also argues that the trusted-third-party network device does not negotiate private IP addresses between the end devices, because network devices 14 and 16 negotiate addresses. PO Resp. 31–32. Patent Owner fails to explain how this argument relates to a claim limitation. Claims 1 and 16 do not require a single device to negotiate, intercept, or determine anything. In any event, Petitioner responds to the argument persuasively and shows that in at least one of Beser’s embodiments, trusted-

structures that are known to those skilled in the art are possible *for the association of the unique identifiers and IP 58 addresses for the second network devices 16.*” Ex. 1007, 11:50–55 (emphases added); *see* Inst. Dec. 18 (discussing and quoting Ex. 1007, 11:47–52); Inst. Dec. 21–22 (discussing association of public IP addresses of 16 and 26). Therefore, in this configuration, Beser’s DNS 30 looks up the public IP 58 addresses of devices 16 and 26 based on a domain name (unique identifier) of terminating device 26—in order to associate the two devices.

third-party network device 30 performs the negotiation. *See* Pet. Reply 11 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs. 6 and 9).

In summary, Beser discloses looking up the private and public IP addresses for end device 26. *See* Ex. 1007, 8:9–15, 11:50–55, 12:5–12, Fig. 4; *supra* notes 16, 17. To make the association, Beser’s DNS 30, a directory service, stores public IP addresses for device 26 under one configured option. *Supra* note 16; Ex. 1007, 11:45–55; *supra* Section II.D (describing Beser); *see also* Inst. Dec. 9 (“Trusted-third-party network 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 device 16 and terminating devices 26) (citing Ex. 1007, 11:32–52); PO Resp. 32 (“*Beser . . .* states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26”) (citing Ex. 1007, 11:50–55). Therefore, Beser discloses that it associates devices 16 and 26 by, among other ways, looking up a private IP address for device 26, and the public IP addresses of one or both of devices 16 and 26, as stored in a database, including a DNS type database, based on the unique domain name for device 26. *See, e.g.*, Ex. 1007, 8:3–20, 11:26–58, 12:28–32, 17:42–49, Ex. 2018 ¶¶ 44–45; notes 16–17; Ex. 1005 ¶¶ 150, 164–66 (DNS operates “much like a file system”), 341–44 (describing well-known DNS functionality as disclosed in Beser and the ’705 patent as providing a look-up function). Patent Owner does not dispute that Beser’s system, including DNS 30, associates the public IP addresses of devices 16 and 26 with the domain name of device 26 and returns a private IP address for terminating device 26. *See* PO Resp. 31–32; Ex. 2018 ¶¶ 44–45.

We adopt Petitioner’s showing regarding the “determining . . . whether” and “request to look up” clauses as summarized above. Based on the foregoing discussion and further discussion below regarding encryption and reasons to combine, Petitioner shows by a preponderance of evidence that Beser discloses the “determining . . . whether” and “request to look up” clauses of claims 1 and 16.

3. Encryption and Reasons to Combine

As noted above, Petitioner provides several reasons explaining why an artisan of ordinary skill would have used end-to-end encryption, as disclosed and suggested by RFC 2401, in Beser’s similar network system, for example, to provide enhanced data security and anonymity in networks having similar topology. *See, e.g.*, Pet. 30–32. Petitioner relies further on RFC 2401 as suggesting encryption of data, by using the IPsec protocol, the same encryption protocol that Beser discloses. *See* Pet. 31–33, 39–40; Ex. 1007, 1:54–56; Ex. 1008, 4, 7, 10; Ex. 1005 ¶¶ 427–28, 431, 437. Petitioner contends that RFC 2401 provides automatic encryption for traffic traveling through security gateways over a public network, and that Beser employs edge routers and similar gateways, thereby at least suggesting encryption for a secure tunnel. *See* Pet. 31; Ex. 1007, 4:7–8, 4:18–29; Ex. 1008 (IPsec), 4–6, 25 (Case 3), 30 (“IPsec processing, e.g., authenticate and encrypt”); Ex. 1005 ¶¶ 434–35. RFC 2401 also describes an IPsec goal as providing “confidentiality (encryption).” Ex. 1008, 4.

In response, Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner. PO Resp. 36–42. Patent Owner contends that Beser teaches away from encryption:

The Institution Decision asserts that *Beser* “recognizes that the use of encryption may cause challenges, [but] also suggests that such problems may be overcome by providing more computer power.” (Decision at 13 (citing Ex. 1007 at 1:60–63).) This position reflects a misunderstanding of *Beser*. If adding computing power to every computational problem was a solution, there would have been no need for *Beser*’s tunneling solution. (Ex. 2018 at ¶ 59.) Indeed, in the passage cited by the Board, *Beser* notes the *problems* with allocating more computing power to encryption, such as “jitter, delay, or the loss of some packets.” (Ex. 1007 at 1:60–65.) *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. (Ex. 1007 at 1:65–67; Ex. 2018 at ¶ 59.)

PO Resp. 37–38.

Patent Owner also contends that *Beser* only “proposes a method of hiding the addresses of originating and terminating devices”:

By hiding the identities of the network devices in this manner, *Beser* touts that its method is able to increase communication security without increasing computational burden. (*Id.* at 2:43–3:14.) Thus, one of ordinary skill in the art would have understood that *Beser* is directed to providing a method for securing communications *other than* encryption. (See Ex. 2018 at ¶ 61.)

PO Resp. 38–39.

Patent Owner explains that “*Beser* also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, *Beser* eschews encryption in favor of hiding the identities within the tunnel.” *Id.* at 40.

According to Patent Owner,

the purpose of the encryption in *Beser* is simply to hide address information on the public network prior to *Beser*’s tunnel establishment, once the tunnel is created, the originating and terminating device information is hidden and encryption would

not only be redundant, it would contravene *Beser*'s express objective of increasing security without increasing computational burden.

Id. (citing Ex. 2018 ¶ 64).

Patent Owner's contentions are not persuasive. Although *Beser* recognizes that the use of encryption may cause challenges, contrary to Patent Owner's characterization of *Beser*, *Beser* suggests that such challenges may be overcome by providing more computer power and/or less quality. See Ex. 1007, 1:60–67. For example, *Beser* teaches that an “increased *strain on computer power* [i.e., as opposed to increased computer power] may result in jitter, delay, or the loss of some packets.” *Id.* at 1:63–64.

As Petitioner persuasively argues,

Beser never states its technique is intended to replace encryption. In fact, *Beser* distinguishes between using encryption to protect the data inside packets and using IP tunnels to hide the true addresses of the end devices, as Patent Owner recognizes. Resp. at 36–37. And Dr. Monroe agreed a person of ordinary skill would have recognized that using a security technique to protect the identities of the parties communicating is not a substitute for using encryption to protect the contents of the communications sent between the parties. Ex. 1066 at 74:4–15; 74:25–75:3.

Pet. Reply 7.

Contrary to Patent Owner's related allegations (see PO Resp. 40), *Beser* does not describe that a hacker could defeat *Beser*'s system, whether it employs data encryption or not. Compare Ex. 1007, 2:1–17 (describing a prior art method of “thwarting the hacker” by “encrypt[ing] before the encapsulation to hide the source IP address” that “due to computer power limitations . . . may be inappropriate for the transmission of multimedia or VoIP packets”), with *id.* at 2:39–40 (“[h]iding the identities may prevent a

hacker from intercepting all media flows between ends”). In other words, Beser’s system uses private addresses hidden in packets so that encrypting data secures the data, and encrypting the addresses further secures the addresses, so that a hacker would be thwarted. To emphasize the point, Beser specifically characterizes some prior art systems as creating “*security problems by preventing certain types of encryption from being used.*” Ex. 1007, 2:23–24 (emphasis added). Therefore, Beser does not discourage encrypting data to make it secure; rather, Beser provides a solution for providing anonymity by using a tunnel technique with or without encryption of data, and if necessary, increasing computer power as needed when encryption for data or otherwise may be desired.

Further regarding teaching away, Beser at most mildly criticizes (tempered by an implied solution) a specific type of tunneling that employs encapsulation, encryption, and VoIP packets—i.e., “due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.” Ex. 1007, 2:15–17. In other words, Beser at least suggests that with adequate power or typical data transmissions, a tunnel (a VPN according to Beser) and encryption would be appropriate for providing security. *See also infra* Section II.E.1 (discussing encryption in a VPN per challenged claims 6 and 21).

As summarized above, notwithstanding Patent Owner’s arguments, Petitioner establishes that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with Beser to encrypt data in order to enhance data security in a tunnel that provides anonymity, based on a determination that a requested target device would have been available for a secure communication. Petitioner also sets forth a persuasive rationale

showing that Beser's combined system includes or suggests using a DNS to help determine that a requested end device is available for secure communications by, among other things, associating that end device with a private IP address. See Ex. 1007, Fig. 1 (depicting private network 20 on the origination end); 11:62–64 (“Private IP 58 addresses are addresses that are reserved for use in private networks that are isolated from a public network such as the Internet.”). Finally, Petitioner sufficiently shows that the combination suggests the determination function as set forth in claim 1, because the combination suggests encrypting all devices listed on the network and/or listing only devices for connection on private networks in Beser's system. We adopt Petitioner's analysis and showing, as summarized above, as our own.

4. Remaining clauses

The Petition establishes that the combination of Beser and RFC 2401 discloses or suggests the remaining limitations of claims 1 and 16, for example, the memory, application program, and processor for providing audio/video communications over the secure link. See Pet. 37–42 (relying *inter alia* on the combined teachings of Beser and RFC 2401 to provide look-up functionality to determine all devices for private connection also are encrypted end-to-end on a secure channel, and relying on Beser's client device that provides multimedia applications on a secure channel); Ex. 1007, 1:54–56, 4:43–52, 8:21–50, 11:26–28; Ex. 1005 ¶¶ 331, 355, 361–363. Patent Owner does not argue with particularity in its Patent Owner Response that the combination of Beser and RFC 2401 fails to disclose or suggest the remaining clauses in claims 1 and 16. Based on further review of the record, we adopt Petitioner's analysis and showing as our own, and determine that

Petitioner establishes that Beser’s system provides the additional recited limitations, including allowing audio/video data in a secure communication link and determining whether the terminating device is a device with which a secure communication link can be established, as required by claims 1 and 16. *See* Pet. 41–42, *see also* Ex. 1007, Abstract (disclosing VoIP secure communications by initiating a tunnel between end devices over a public network), Fig. 1; *supra* Section II.D (summarizing Beser).

Based on the foregoing discussion and record, Petitioner shows by a preponderance of evidence that the combination of Beser and RFC 2401 would have rendered claims 1 and 16 obvious.

E. Dependent Claims 1, 6, 7, 13, 21, 22, and 28

1. Claims 6 and 21

Claims 6 and 21 respectively depend from claims 1 and 16 and require the secure communication link to be a VPN link. Petitioner generally relies on its explanation above in which the combined system of Beser and RFC 2401 create a VPN based on anonymity and encryption over Beser’s tunnel. *See* Pet. 23–24, 47–48 (citing Ex. 1005 ¶ 138); Pet. Reply 13–16 (citing Ex. 2008, 25 (noting that IPsec, as defined by RFCs, can be used to establish VPNs)).¹⁷

Patent Owner contends that Beser criticizes a VPN as “[a] form of tunneling [that] may be inappropriate for the transmission of multimedia or VoIP packets’ . . . , immediately before introducing *Beser’s* tunnel as a

¹⁷ *See Cisco*, 767 F.3d at 1318–19 (construing VPN link and secure communication link interchangeably, and holding that “the term [‘secure communication link’] should be construed as “a direct communication link that provides data security *and anonymity*”).

solution to the problems posed by VPNs for VoIP.” PO Resp. 43 (quoting and citing Ex. 1007, 2:6–17, 2:43–66). Therefore, according to Patent Owner, Beser “expressly teaches that its tunnel is not a VPN communication link.” *Id.* (citing Ex. 2025 ¶ 60).

Patent Owner’s characterization fails to address the combination as advanced by Petitioner, and it mischaracterizes Beser’s teachings. *See* Pet. 47–48. As to the first point, Petitioner contends that Beser’s tunnel provides anonymity over a public network, and that the combination with RFC 2401 provides direct end-to-end encryption. *Id.* A VPN reads on this combined system according to a claim construction addressed in *Cisco* (note 17) and embodiments disclosed in the ’705 patent disclosure. *See* Ex. 1050, Fig. 26 (VPN system), Fig. 33 (same), 41:6–15 (a VPN employs a hopping regime (i.e., providing anonymity)); *see also* Ex. 1005 ¶¶ 136–38 (discussing a broader construction of VPN than that addressed in *Cisco* as consistent with the ’705 patent Specification, including Figure 33). Patent Owner does not argue that the claimed VPN according to *Cisco* (note 17) does not read on the combined system of Beser and RFC 2401.

As to the second point, as Patent Owner states, Beser discloses that “[o]ne method of thwarting [a] hacker is to establish a Virtual Private Network (‘VPN’) by initiating a tunneling connection between edge routers on the public network.” PO Resp. 42–43 (quoting Ex. 1007, 2:6–8). Beser then discusses problems with such a VPN if it employs encryption without providing enhanced power, but Beser does not state that a VPN has insurmountable problems, if any, or that Beser’s tunnel is not a VPN. For example, as discussed above, Beser teaches that “[o]nce again, *due to computer power limitations*, this *form* of [VPN] tunneling [that uses

encryption] may be inappropriate for the transmission of multimedia or VoIP packets.” Ex. 1007, 2:15–17. As discussed above, Beser solves the hacking problem by providing private network addresses in a tunnel (as opposed to encryption and mere encapsulation), and Beser also teaches that additional computer power would solve any problems arising from encryption. Therefore, assuming that a VPN communication link requires encryption, the combination of Beser and RFC 2401 suggests that feature and would have rendered obvious a VPN communication link required by claims 6 and 21.

2. Claims 7 and 22

Claims 7 and 22 further specify that the domain name is a “secure domain name.” Petitioner contends that Beser and RFC 2401 would have rendered obvious a secure domain name. According to Petitioner,

Beser shows that the unique identifier can be a domain name, an email address, or an E.164 number, and that if the unique identifier corresponds to a secure destination, the trusted-third-party network device will automatically negotiate an IP tunnel between the end devices by negotiating private IP addresses that will be used to transmit data between these end devices across a public network. Ex. 1007, 7:64–8:20, 10:38–41, 10:55–11:5, 10:66–11:2; Ex. 1005 ¶¶ 346, 357, 368, 371. Beser thus shows a “secure domain name” because the unique identifier can be a name that corresponds to a secure computer network address (*i.e.*, the private IP address of the terminating end device). Ex. 1005 at ¶¶ 357, 361–63.

Pet. 48–49.

Petitioner adds that Beser’s trusted-third-party network device can require “encryption or authentication” of an originating device before processing a request to initiate a tunneling association, showing or at least

suggesting that any private IP address would be for a secure domain name. *Id.* at 49 (citing Ex. 1007, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 429–30).

Patent Owner responds that “*Beser* does not disclose any nonstandard domain names that cannot be resolved by a conventional DNS.” PO Resp. 44 (citing Ex. 1007, 10:38–41; Ex. 2018 [¶] 67). Patent Owner contends that a “secure domain name” should be construed as a “*non-standard domain name* that corresponds to a secure computer network address and *cannot be resolved by a conventional domain name service (DNS)*.” *Id.*

These arguments turn on Patent Owner’s narrow claim construction that the record does not support and we do not adopt. *See supra* Section I.D.3. Patent Owner does not rebut Petitioner’s showing that *Beser* satisfies our adopted claim construction. As Petitioner contends in the quoted passage above, *Beser* discloses or suggests using a domain name that corresponds to a secure device—“a name that corresponds to a secure computer network address,” according to our adopted claim construction. These secure devices exist on private networks, which are relatively secure, according to *Cisco* and *Beser*, especially where authentication or encryption may be required, and anonymity is required. *See* Ex. 1007, Fig. 1; 4:22–24 (edge routers route packets over a public network to private networks), 11:62–65 (“Private IP 58 addresses are addresses that are reserved for use that are isolated from a public network such as the Internet.”), 1:18–20 (“Companies who cannot afford a private network often transfer sensitive corporate information over the Internet”); *Cisco*, 767 F.3d 1321 (*VirnetX* presented evidence that “the virtual private network extends[s] from the client computer to the target computer . . . because it’s encrypted on the insecure paths, and it’s secure within the corporate network”). In addition,

they would be determined to be secure by virtue of having end-to-end encryption and listed for connection as a secure device according to Petitioner's obviousness challenge that involves creating a private network in view of RFC 2401's teachings. *See* Pet. 29–30, 44–45.

Assuming, for the sake of argument, that Patent Owner's narrow claim construction applies (*see supra* Section I.D.3), like the '705 patent's disclosed system, Beser's system resolves domain names by a combined conventional and non-conventional DNS look-up process, because, as explained above, the system includes a negotiation process to look up private secure addresses. Ex. 1007, Figs. 4–5; Section II.D (describing Beser); Section II.G.2 (describing Beser's look-up with respect to claim 1). Beser also does not restrict names to conventional domain names and services: "many more unique identifiers and trusted-third-party network devices are possible." *Id.* at 11:57–58; *see also* 10:66–11:2 (unique identifiers include telephone numbers, employee numbers, or "any other possible unique identifier . . . included in the payload of an IP"); Pet. 29–30, 44. Therefore, Beser discloses, or at least suggests, using a non-standard domain name associated with a secure device and satisfies both Petitioner's and Patent Owner's claim constructions. *See supra* Section I.D.3.

Stated another way, using non-standard domain names and private IP addresses for devices on private networks (in combination with RFC 2401's suggestion to provide encryption on private networks), as Petitioner alleges, shows that non-standard domain names cannot be resolved by a conventional DNS, if we follow Patent Owner's logic underlying its claim construction—i.e., involving the dependent interplay between a "non-

standard” domain name allegedly precluding a “conventional” DNS look-up of that name as discussed above in Section I.D.3.

Patent Owner also argues that the trusted-third-party network device does not negotiate private IP addresses between the end devices, because “network devices 14 and 16 negotiate addresses.” PO Resp. 44. Patent Owner’s argument tracks its argument for claims 1 and 16 and fails to explain how this argument relates to a claim limitation. Claims 1, 7, 16, and 22 do not require a single device to negotiate, intercept, or determine anything. In any event, as discussed with respect to claims 1 and 16, Petitioner responds to the argument persuasively and shows that one of Beser’s embodiments includes trusted-third-party network device 30 performing negotiation. See Pet. Reply 11 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs. 6 and 9).

3. Claims 13 and 28

Claims 13 and 28 respectively depend from claims 3 and 16 and recite that “the target device is a server.” Claim 3 depends from claim 1 and further limits the client device (as a phone). Petitioner contends that a skilled artisan would have understood from Beser’s disclosure of target devices 26 as being accessible via a domain name, and including “Web-TV sets and decoders, interactive video-game players, or personal computers running multimedia applications. . . . [.] would suggest to a person of ordinary skill in the art that the terminating end device could be a server.” Pet. 54 (citing Ex. 1007, 4:47–49, 10:39–41, 10:55–11:5; Ex. 1005 ¶¶ 160–66, 327).

In response, Patent Owner acknowledges that Beser’s target devices 26 can be “multimedia devices,” but contends this fails to show they are

servers. PO Resp. 45. Patent Owner also contends that just because “the terminating device 26 (the alleged target device) can *connect to* a server does not disclose, inherently or otherwise, that the terminating device itself is a server.” *Id.* Patent Owner also argues that Beser does not suggest a server, because Petitioner’s expert relies on name servers disclosed in Beser as related to trusted-third-party device 30. *See id.* at 46.

In the Institution Decision, we made the following preliminary findings:

Dr. Tamassia generally describes Beser’s DNS as functioning in a known manner and providing services that track the location of “resources or computers” from clients by looking up address information. Ex. 1005 ¶ 342. Moreover, Beser explicitly states that “the ends of the data flow may be other types of network devices,” including a wide variety of devices, and “the present invention is not restricted to telephony or multimedia devices.” *See* Pet. 53–54 (quoting Ex. 1007, 4:53–54, citing 4:14–18, 43–54). As Patent Owner acknowledges, Beser discloses servers. Prelim. Resp. 25–26. Claims 13 and 28 do not specify any special function for the claimed servers.

Inst. Dec. 17.

Patent Owner’s arguments fail to rebut Petitioner’s showing regarding the obviousness of using servers as target devices. Beser discloses “personal computers” that include, but are not restricted to, running multimedia, audio, or video services, as target devices 26. Ex. 1007, 4:49–52. These computers provide services to originating devices 24. *See* Ex. 1007, Fig. 1. As Petitioner contends,

[a] person of ordinary skill in the art would have understood that where originating device 24 is a Web-TV, terminating device 26 is a Web-TV **server** that sends television content to the client. Ex. 1005 at ¶327; *id.* at ¶¶160–166. Similarly, that person would have understood a web browser to be a type of multimedia

application, and that a web browser downloads content from a server. *Id.*

Pet. Reply 18.

4. Summary, Claims 1, 6, 7, 13, 21, 22, and 28

Petitioner has the burden of persuasion to show the unpatentability of the challenged claims. We adopt Petitioner's showing and analysis, as summarized above, as our own. Based on the foregoing discussion, and a review of the record, Petitioner demonstrates by a preponderance of evidence that the combination of Beser and RFC 2401 would have rendered claims 1, 6, 7, 13, 21, 22, and 28 obvious.

*F. Dependent Claims 2–5, 8–12,
14, 15, 17–20, 23, 25–27, 29, and 30*

In the Institution Decision, we initially determined that Petitioner shows that the combination of Beser and RFC 2401 would have rendered challenged dependent claims 2–5, 8–12, 14, 15, 17–20, 23, 25–27, 29, and 30 obvious. *See* Inst. Dec. 18–19; Pet. 43–46, 49–53. In response, Patent Owner relies on arguments presented for patentability of claims 1, 6, 7, 13, 21, 22, and 28. *See* PO Resp. 47.

Petitioner has the burden of persuasion to show the unpatentability of the challenged claims. We have reviewed both parties' arguments and supporting evidence, including the disclosure of both references and the testimony of Dr. Tamassia and Dr. Monroe, and we agree with Petitioner's analysis and adopt it as our own. Thus, we determine that Petitioner has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found dependent claims 2–5, 8–12, 14, 15, 17–20, 23, 25–27, 29, and 30 over Beser and RFC 2401.

G. Dependent Claim 24

In the Institution Decision, we initially found and determined that Petitioner shows that the combination of Beser, RFC 2401, and Brand would have rendered obvious claim 24. *See* Inst. Dec. 18–19; Pet. 54–56. In response, Patent Owner relies on arguments presented for patentability of claim 16. *See* PO Resp. 47.

Petitioner has the burden of persuasion to show the unpatentability of the challenged claims. We have reviewed both parties’ arguments and supporting evidence, including the disclosure of the three references and the testimony of Dr. Tamassia and Dr. Monroe, and we agree with Petitioner’s analysis and adopt it as our own. Thus, we determine that Petitioner has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found dependent claim 24 obvious over the combination of Beser, RFC 2401, and Brand.

III. PATENT OWNER’S MOTION TO EXCLUDE

Patent Owner seeks to exclude Exhibits 1001–1004, 1006, 1009–1011, 1013–1041, 1043–49, 1051–54, 1060, 1063–65, and 1071, and portions of Exhibit 1005. Paper 30, 1. As movant, Patent Owner has the burden of proof to establish that it is entitled to the requested relief. *See* 37 C.F.R. § 42.20(c). For the reasons stated below, Patent Owner’s Motion to Exclude is *dismissed* as *moot* in part and *denied* in part.

1. Exhibits 1060 and 1063–65

Patent Owner moves to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 30, 2. Exhibit 1060 is a declaration originally submitted in litigation before the International Trade Commission. Ex. 1060. It contains testimony from Sandy Ginoza, a representative of IETF, in

support of Petitioner’s contention that RFC 2401 qualifies as a printed publication as of November 1998. *Id.* Exhibit 1063 is a “transcript of Ms. Ginoza’s February 8, 2013 deposition that was taken as part of the ITC action.” Paper 30, 2 (quoting Paper 17, 5–6). Exhibits 1064 and 1065 are both magazine articles dated 1999 that relate to the same issue. *See* Paper 17, 7–8. All four exhibits were entered into the record after deciding upon Petitioner’s Motion to Submit Supplemental Information Pursuant to 37 C.F.R. § 42.123(a). *See* Paper 14; Paper 17.

Because we do not rely on any of these Exhibits to decide the issue of whether RFC 2401 qualifies as a printed publication, we dismiss the motion as to these Exhibits as moot.

*2. Exhibits 1001–04, 1006, 1009–11,
1013–41, 1043–49, 1051–54, and 1071*

Patent Owner seeks to exclude the above-listed exhibits as lacking relevance and “one or more” is inadmissible hearsay. Paper 30, 1, 5–6. Because we do not rely on any of the exhibits listed above, we dismiss this request as moot.

3. Portions of Exhibit 1005

Patent Owner seeks to exclude portions of Dr. Tamassia’s testimony in Exhibit 1005 as lacking relevance because they focus on Aventail (an alleged prior art reference not used by Petitioner in this proceeding). *See* Paper 30, 6. Because we do not rely on any of the paragraphs of Exhibit 1005 that deal with Aventail, we dismiss this request as moot.

4. Exhibit 1036

Patent Owner moves to exclude Exhibits based on the following argument: “Exhibits 1001–1004, 1006, 1009–1011, 1013–1041, 1043–1049, 1051–1054, 1060, 1063–1065, and 1071 because *one or more of these*

exhibits includes evidence that is inadmissible hearsay or the evidence in these exhibits is irrelevant to the instant proceeding.” Paper 30, 1 (emphasis added). Patent Owner also argues as follows: “Exhibits 1001–1004, 1006, 1009–1011, 1013–1041, 1043–1049, 1051–1054, and 1071 should be excluded because they lack relevance.” *Id.* at 5.

As indicated in the first above-quoted argument, Patent Owner does not argue specifically that Exhibit 1036 includes evidence of hearsay, because that argument applies to “one or more” of the other listed Exhibits. Furthermore, Patent Owner does not explain why anything in Exhibit 1036 includes hearsay. *See* Paper 30, 1. Accordingly, Patent Owner fails to meet its burden on its Motion to Exclude Exhibit 1036 based on hearsay. *See* 37 C.F.R. § 42.20(c).

Patent Owner’s second above-quoted argument is based on an asserted lack of relevance as to all the listed Exhibits, including Exhibit 1036. Patent Owner does not explain why Exhibit 1036 is not relevant. Therefore, Patent Owner fails to carry the burden on its Motion to Exclude Exhibit 1036. *See* 37 C.F.R. § 42.20(c). Furthermore, as discussed above in Section II.C, Dr. Tamassia relies on Exhibit 1036, and it provides evidence of procedures used in the publication of RFC documents. Therefore, Exhibit 1036 is relevant to show the public availability of RFC 1041. Accordingly, based on the foregoing discussion, we *deny* the Motion to Exclude Exhibit 1036.

IV. CONCLUSION

Petitioner has demonstrated, by a preponderance of the evidence, under 35 U.S.C. § 103(a), the unpatentability of claims 1–23 and 25–40

based upon the combination of Beser and RFC 2401, and of claim 24 based on the combination of Beser, RFC 2401, and Brand.

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that claims 1–30 of U.S. Patent No. 8,560,705 B2 are unpatentable;

FURTHER ORDERED that Patent Owner’s Motion to Exclude is *dismissed as moot* with respect to Exhibits 1001–1004, 1006, 1009–1011, 1013–35, 1037–41, 1043–1049, 1051–1054, 1060, 1063–1065, and 1071 and is *denied* with respect to Exhibit 1036;

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

IPR2015-00870
Patent 8,560,705 B2

PETITIONER:

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

PATENT OWNER:

Joseph E. Palys
Naveen Modi
Daniel Zeilberger
Chetan R. Bansal
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com
chetanbansal@paulhastings.com

Jason Stach
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.
jason.stach@finnegan.com

.