

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00871
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. Pet. 2–3. After VirnetX Inc., Patent Owner, filed a Preliminary Response (Paper 6, “Prelim. Resp.”), we instituted an *inter partes* review of claims 1–30 (Paper 8, “Institution Decision” or “Inst. Dec.”). Inst. Dec. 2.

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.*, IPR2015-00870 (PTAB Sept. 28, 2016) (Paper No. 39, “’870 FWD”) (generally “’870 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 “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 . . . IP address ‘hopping’ features,” (changing IP addresses based upon an agreed upon algorithm) described in the ’705 patent, “such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted.” *See 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 Aventail¹ (Ex. 1009–11), RFC 2401² (Ex. 1008), and RFC 2543³ (Ex. 1013), and claim 24 as unpatentable based on the combination of Aventail (Ex. 1009–11), RFC 2401 (Ex. 1008), RFC 2543 (Ex. 1010), and Brand (Ex. 1012).⁴ Inst. Dec. 21.

II. ANALYSIS

A. 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

¹ Exhibits 1009–1011 correspond to manuals that collectively describe an Aventail Connect client and ExtraNet Server software application. We refer collectively to the three manuals as “Aventail” unless otherwise noted. See Aventail Connect v3.01/v2.51 Administrator’s Guide (Ex. 1009), Aventail Connect v3.01/v2.51 User’s Guide (1996–1999) (Ex. 1010), and Aventail ExtraNet Center v3.0 Administrator’s Guide (NT and UNIX) (“Aventail ExtraNet Admin. Guide”) (Ex. 1011).

² S. Kent and Randall Atkinson, RFC 2401, *Security Architecture for the Internet Protocol*, Network Working Group, Request for Comments (Nov. 1998).

³ Handley et al., RFC 2543, *SIP: Session Initiation Protocol*, Network Working Group, Request for Comments (Mar. 1999).

⁴ U.S. Pat. No. 5,237,566 (Aug. 17, 1993).

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 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. 9–10. 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.

Similar to its position in the ’237 IPR proceeding, Patent Owner states in the instant proceeding that “no construction [is] necessary.” PO Resp. 4; ’237 PO Resp. 23 (“no construction is necessary”). 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, performing an evaluation on it related to establishing a secure communication link." PO Resp. 4; '237 PO Resp. 23.

According to Patent Owner 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." '237 PO Resp. 25. Patent Owner's arguments are similar in material respects in the instant proceeding. 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. 4–5.⁵

The arguments and record shows 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 "a determination is made as a result of the request [to look up an IP address] that the target device is a device with which a secure communication link

⁵ 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) (citation omitted).

can be established”) (addition by Patent Owner). 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. 27–30; ’237 PO Resp. 26, 29–30.

The parties agree that “interception of a request” (at least) involves “receiving a request” at some intermediate device. See PO Resp. 4; Pet. 9–10. Patent Owner’s proposed construction does not create any distinction 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 5. In essence, Petitioner’s construction captures the notion of interception as disclosed in the ’705 patent, by requiring receiving to “pertain” to another entity.

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, as set forth in 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 15.⁶

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).

The Specification supports this interpretation:

If access to a secure 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 structure) of secure sites is sufficient to constitute a determination of availability.

⁶ We consider the phrase “in response to the request” in the ’237 IPR to have been omitted inadvertently from the claim construction in that case without consequence.

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. 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 the related ’481 *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 final written decision, 13–14 (same claim construction).⁷ 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.* 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”

⁷ As indicated above, reference is to *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481 (“’481 IPR”), slip op. at 8 (PTAB Sept. 3, 2014) (Paper 11) (“’481 institution decision”); and ’481 IPR, slip op. at 13–14 (PTAB Aug. 24, 2015) (Paper 35) (“’481 final written decision”).

corresponds to 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.* at 22–23 (citing Ex. 2018 ¶¶ 36–38).⁸ Dr. Monroe contends, *inter alia* (see note 8), 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).

Patent Owner further contends it disclaimed Petitioner’s proposed construction in a now completed *inter partes* reexamination of a related patent. PO Resp. 23 (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 11, 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

⁸ 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.

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.” Ex. 1050, 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 secure DNS using a conventional look-up function not to return the secure domain names contemplated by the invention. The 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. Similarly, rather than a *conventional* domain name not returning a secure address based solely on the name, the Specification states that a “DNS *proxy*” returns a “host-unknown” “[i]f the user had requested lookup 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 II.A.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 communication services 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 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. *See also supra* note 5 (conventional DNS part of disclosed embodiments). 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 ¶¶ 164–66 (“much like a file system”), 341–44 (describing well-known DNS functionality as disclosed in 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 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). 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.* at 23; *see also id.* at 24 (citing Ex. 2017, 4); *accord* Ex. 2016, 6 (Patentee arguing during prosecution that “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, for some embodiments, other possible 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”).⁹

⁹ 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.

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 9) 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 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 in the related '870 IPR 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.**" '870 Pet. Reply 17 (citing '870 Ex. 1069, 9).¹⁰ 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

¹⁰ Exhibit 1069 is the same in this IPR and in the '870 IPR.

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)).¹¹ The record here supports 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, the 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

¹¹ The district court case cited in the ’481 IPR involved construction of a different term: “secure domain name service.” See ’481 Ex. 1018, 17–18. The Board 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”).

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."

4. Virtual Private Network Link and Secure Communication Link

Claims 1 and 16 recite a "secure communication link." Claims 6 and 21 recite a "virtual private network link" ("VPN link)." Patent Owner contends that a "virtual private network link" or VPN link requires a network and a direct connection. PO Resp. 18–21. Patent Owner similarly contends that "secure communication link" also requires a direct connection. PO Resp. 5–6 (citing Ex. 2018 ¶¶ 15–26). Patent Owner proposes that a secure communication link means "[a] direct communication link that provides data security through encryption." PO Resp. 5. Patent Owner construes a "virtual private network link" as "a path between two devices in a virtual private network." *Id.* at 15.

Disagreeing with Patent Owner, and citing, *inter alia*, the Board's claim construction in the '237 IPR and '481 IPR, Petitioner proposes that the terms "secure communications link" and "VPN link" each mean "a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." See Pet. 11–12 (citing '237 IPR institution decision, 10 (PTAB May 14, 2014) (Paper 15), 14–15 (citing '481 IPR institution decision, 6–7); Pet. Reply 3 (arguing that

prosecution history and the '705 patent do not show that a secure communication and VPN link requires a “direct” communication).

Regarding the alleged “network” requirement, Petitioner points to the '705 patent Specification, which discloses that “software module 3309 accesses secure server 3320 through VPN communication link 3321.” Pet. 14 (quoting Ex. 1050, 51:66–67; Fig. 33). Petitioner also explains that with respect to Figure 33, “communication link 3321 is shown as only the portion of the path between computer 3301 and server 3320 that is over network 3302.” *Id.* (citing Ex. 1005 ¶ 137). Figure 33 and relevant descriptions thereof reveal a mere communications link 3321 that connects between ISP 3303 and server 3320, without requiring a network of other devices, as Petitioner contends. *See* Ex. 1050, 51:66–67, Fig. 33. Therefore, the record does not support a requirement for a “network” within a VPN link.

Regarding the alleged “direct” requirement, Petitioner argues the inclusion of “direct” adds an additional limitation that the Board previously rejected in the related '481 IPR. Pet. Reply 3 (citing '481 final written decision, 10). Petitioner also contends that the '705 patent Specification describes secure communication links that traverse firewalls, edge routers, and proxies between end devices in a connection. *Id.* (citing Ex. 1050, 33:48–34:12, 49:19–23, 53:18–59, 55:34–46). The '705 patent also discloses that each router may perform decryption of packet information along the path. Ex. 1050, 9:66–1016.

The Specification does not show clearly how different edge routers, intervening routers, or other embodiments require a “direct” connection, or show what the term “direct” means. In the absence of such a special definition or other consideration, “limitations are not to be read into the

claims from the specification.” *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993). Patent Owner alleges that it disclaimed the term in a clear fashion during prosecution of related patents, but fails to explain what “direct” means. *See* PO Resp. 8–12 (citing Ex. 2012, 8), 18–19 (citing Ex. 2006, 6–9; Ex. 2011, 7).

Patent Owner also argues that in the *Cisco* litigation, in district court, Petitioner argued that for the “direct” requirement and our reviewing court agreed with Petitioner. PO Resp. 9–10 (citing *VirnetX Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317 n.1 (Fed. Cir. 2014); Ex. 2002, 5–7, 10). Patent Owner also contends that the Federal Circuit construed the terms to require the “direct” component. *See id.* at 10 (citing *Cisco*, 767 F.3d at 1319). Specifically, *Cisco* construed “secure communication link” to mean “a direct communication link that provides data security and anonymity.” *Cisco*, 767 F.3d at 1319 (emphasis omitted).

Not requiring the claims challenged claims to include an implicit “direct” communication does not contradict *Cisco*’s construction. In contrast to the broadest reasonable interpretation standard employed by the Board for an unexpired patent, the Federal Circuit does not employ that standard when reviewing a district court’s construction. *See In re Rambus, Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012) (contrasting the Board’s review of expired patents, which is “similar to that of a district court’s review,” with the Board’s review of unexpired patents, which involves the broadest reasonable interpretation standard); *Cuozzo*, 136 S. Ct. at 2142. In addition, *Cisco* indicates that the parties did not dispute the “direct” requirement in *Cisco*, and the court simply adopted the requirement because it was not in dispute for purposes of the appeal. *See Cisco*, 767 F.3d at 1317–19 & n.1

(no discussion of a controversy about the “direct” requirement). As indicated above, the ’705 patent Specification does not require a direct link and Patent Owner does not explain clearly how to interpret “direct” on this record.

Patent Owner lists examples that allegedly encompass a direct link, but the record fails to illuminate how to interpret “direct.” See PO Resp. 9 (“In each of these embodiments, the ’0705 patent specification discloses that the link traverses a network (or networks) through which it is simply passed or routed via various network devices such as Internet Service Providers, firewalls, and routers.” (citing Ex. 1050, 40:13–16, 41:5–8, 49:8–10, 49:16–31, Figs. 24, 26, 28, 29, 33; Ex. 2018 ¶¶ 21–24)). In addition to Patent Owner’s characterization of “direct” as including various intervening devices along a path between two devices, the ’705 patent also describes processing the packets at each router along the link to decrypt the packets. See Ex. 1050, 9:66–10:16. It also describes connections through an “Internet, through an ISP 3303,” through an “edge router, and through a “load balancer that distributes packets across different transmission paths.” See Ex. 1050, 6:11–12, 49:20–23. The ’705 patent fails to shed light on what “direct” means.

During a reexamination of related U.S. Patent No 6,502,135 (the “’135 patent”), Patent Owner made several arguments and contended in the district court that its various prosecution arguments did not amount to an unequivocal disclaimer.¹² See Ex. 2011, 7; Ex. 2002, 5–6. In one argument,

¹² In the district court litigation cited by Patent Owner, as we noted in the Institute Decision (Paper 8, 19–20 n.6), notwithstanding the district court’s findings, according to the defendant’s summary of arguments by Patent

Patentee argued that “Aventail Connect’s falsification of [i.e., a false DNS response] the network information would prevent the correct transfer of data,” and “[t]hus, Aventail has not been shown to disclose a VPN.” Ex. 2011, 7. In another argument, Patentee described a scenario in which a VPN requires two public computers X, Y to be able to communicate with two private computers A, B “without establishing a separate SOCKS connection,” indicating (perhaps) that a VPN requires all four “to be a part of the same VPN.” *See id.* at 6. Patentee also argued that Aventail did not disclose a VPN “because computers connected according to Aventail do not communicate directly with each other.” *Id.* at 7.

Setting aside the first two arguments, and noting that the ’135 patent reexamination examiner did not rely explicitly on any of the arguments (*see* note 12) in the reexamination proceeding, Patentee failed to clarify what “directly” means, and as another example, argued that Aventail’s SOCKS (ExtraNet) server merely “relays” data “to a target computer on a private network,” and “[t]he client cannot open a connection with the target itself. . . . Instead the client computer and target computer are deliberately separated by the intermediate SOCKS server.” Ex. 2011, 7. But as

Owner in the district court, Patent Owner argued that *it did not* make a clear disclaimer at the PTO disavowing the scope of a VPN regarding the direct requirement. *See* Ex. 2002, 5–6; *see* Prelim. Resp. 38 (citing Ex. 2002, 5). The examiner confirmed claims 1, 3, 4, 6–10, 12, and 18 in the related ’135 patent over Aventail, because besides the copyright date, the “request did not set forth any further evidence of the date of publication” as to Aventail. *See* Reexam. Cont. No. 95/001,269, Action Closing Prosecution, 3 (June 16, 2010), Right of Appeal Notice, 4 (Oct. 29, 2010). Prior to that determination, the examiner found that Aventail anticipated claims 1, 3, 4, 6–10, 12, and 18. *See* Reexam. Cont. No. 95/001,269, Office Action (Jan. 15, 2010).

explained above, the disclosed routers and edge routers in the '705 patent also separate targets and clients, and also relay packet information (and decrypt packets), and Patent Owner now includes routers and other server devices as devices within its claim construction that provide direct connections. Similarly, as described above, the '705 patent requires the proxy to “open a connection.” *See, e.g.*, Ex. 1050, 40:6–13 (“proxy . . . intercepts all DNS look up functions”). Furthermore, in *Cisco*, the court affirmed a finding of infringement even though the infringing product included intermediate “VPN servers, VPN authentication servers, proxy servers, and firewalls.” *Cisco*, 767 F.3d at 1322. In other words, Patentee did not make precise and clear prosecution disclaimers that present a sufficiently clear line of demarcation as to what “direct” means.

During the Oral Hearing of this trial, the panel asked Patent Owner “for a simple definition of ‘direct’” and Patent Owner stated that it “can’t come up with exact words,” but “the crux of direct is direct addressability.” Tr. 42:21–43:2. But when asked “So, that’s the definition of direct is that you have to have the destination in the packet? . . . You have to have the destination address in the packet header, is that what ‘direct’ means?” Patent Owner replied, “No Your Honor, I mean, I think there are many ways.” *Id.* at 42:14–19. In a preceding explanation, Patent Owner stated that the disclosed packets “are routed to each immediate routers, for instance, but they’re addressed directly to final destination.” *Id.* at 42:11–13.

This explanation during the Oral Hearing comports with the cited prosecution history only to the extent that it shows no clear disclaimer occurred. The Oral Hearing “direct addressability” explanation also appears

to be a shift from the “termination” or “relay” alleged disclaimer arguments discussed above. In other words, the Oral Hearing arguments further exemplify that any alleged disclaimer made during prosecution lacks the requisite precision. Furthermore, the ’705 patent states that “[t]he address that is returned need not be the actual address of the destination computer,” implying that the ’705 patent does not require direct addressability in each packet. *See* Ex. 1050, 40:24–25.

Moreover, during the district court litigation, Patent Owner omitted any proposal to include a “direct” requirement in its claim construction proposals. Ex. 2002, 2, 7. In sum, Patent Owner originally contended in cited district court litigation that it did not make a clear disclaimer during prosecution, at least one cited reexamination examiner initially found that Aventail anticipates similar claims in the ’135 patent, and the parties simply appeared to have agreed on a direct requirement during litigation (at least on appeal to the Federal Circuit in *Cisco*). On this record and in this proceeding, the public should not be bound to such a construction under a broadest reasonable construction. *See 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.”).

The patents at issue in *Cisco* have common descriptions to the ’705 patent. *See Cisco*, 767 F.3d at 1313.¹³ In *Cisco*, the court found that “[b]oth the claims and the specification of the ’151 patent make clear that encryption

¹³ The patents in *Cisco* included U.S. Patent Nos. 6,502,135 (“’135 patent”), 7,418,504 (“’504 patent”), 7,490,151 (“’151 patent”), and 7,921,211 (“’211 patent”).

is a narrower, more specific requirement than security.” *Id.* at 1323 (citing a passage in the ’151 patent at 1:49–50 (“Data security is usually tackled using some form of data encryption.”)).¹⁴ This passage, relied upon by the Federal Circuit in its construction, also appears in the ’705 patent. *See* Ex. 1050, 1:57–59.

In the ’237 final written decision, the Board noted the Federal Circuit’s construction of “secure communications link” in *Cisco* and construed the term as meaning “a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of anonymity, authentication, or encryption.” ’237 FWD 8. In the ’481 IPR, the Board similarly interpreted “virtual private network communication link” to mean “a secure communication link that includes a portion of a public network.” ’481 FWD 7.

In making the determination in the ’237 case, the Board noted that *Cisco* determined “encryption is a narrower, more specific requirement than security,” based on the same disclosure here as the patent at issue in *Cisco* that “[d]ata security is *usually* tackled using some form of data encryption.” *See* ’237 FWD 6 (quoting *Cisco*, 767 F.3d at 1323 and patents under challenge). Therefore, under a broadest reasonable interpretation, a “secure communications link” may include encryption or other forms of security, including anonymity.

¹⁴ In *Cisco*, the court also cited testimony at the district court that showed that a direct connection does not preclude intervening routers, firewalls, and similar services or devices on networks such as the Internet (i.e., between the requesting client and target host). *See Cisco*, 767 F.3d at 1320.

Based on the foregoing, we adopt Petitioner’s construction of a secure communication link, but as in the ’481 IPR, slightly modify the construction of a VPN link to mean “a secure communication link that includes a portion of a public network.” We also adopt and incorporate our analyses in the ’237 FWD and ’481 FWD.

B. 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 knowledge “either through several years of practical working experience or through education and training” or some combination of both. Ex. 1005 ¶ 148.

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.

*C. Tamassia Declaration*¹⁵

Patent Owner argues that the entirety of Dr. Tamassia’s declaration should be given little or no weight because “he failed to consider, let alone opine on, how any of the claim features are disclosed in asserted references.” PO Resp. 43. Petitioner responds that Dr. Tamassia has “offered probative testimony on many of the factual inquiries underpinning an obviousness analysis” that “can certainly ‘assist the trier of fact to understand the evidence or determine a fact in issue.’” Pet. Reply 13 (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 14.

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

¹⁵ We address Patent Owner’s motion to exclude certain paragraphs of Exhibit 1005 in a separate section, below.

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. 44. 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:

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.

*D. Prior Art Printed Publication Status of
Aventail, RFC 2401, and RFC 2543¹⁶*

Patent Owner asserts that Petitioner has not sufficiently established that Aventail (PO Resp. 47–51), RFC 2401, and RFC 2543 qualify as printed publications as of their alleged publication dates. *See* PO Resp. 46–60. 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). 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., LLC v. AOL Inc.*, 752 F.3d 1358, 1364 (Fed. Cir. 2014). 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).

¹⁶ We address Patent Owner's motion to exclude exhibits relating to whether Aventail Connect, RFC 2401, and RFC 2543 were publicly available before the critical date in a separate section, below.

1. Aventail

The Petition cites the declarations of James Chester (“Chester Declaration,” Ex. 1022), Christopher Hopen (“Hopen Declaration,” Ex. 1023), and Michael Fratto (“Fratto Declaration,” Ex. 1043), to support its allegation that Aventail “was distributed to the public without restriction no later than January 31, 1999.”¹⁷ Pet. 17–19. Petitioner asserts Aventail is prior art under 35 U.S.C. § 102(b). Pet. 18.¹⁸ Petitioner filed Exhibits 1057–1059 as supplemental information to support its contention about Aventail. See Paper 14.¹⁹ Patent Owner filed a and filed a Motion to Exclude Exhibits 1022, 1023, 1043, and 1057–59 as hearsay as discussed further below. See Paper 30, 2–6.

¹⁷ Exhibits 1022 and 1023 indicate they were filed originally in Reexam. Control No. 95/001,697 requesting reexamination of U.S. Patent No. 7,490,151. See also Pet. Attachment B (Exhibit list). Exhibit 1043 indicates it was filed originally in Reexam. Control. No. 95/001,682 requesting reexamination of U.S. Patent No. 6,502,135. See also *id.* (Exhibit list); Pet. 18 (citing Reexam. Control. No. 95/001,682 for the “declarations”).

¹⁸ Petitioner alleges the effective filing date is no earlier than February 15, 2000. Pet. 7–8. Patent Owner does not dispute the allegation in this proceeding. Petitioner’s supporting evidence includes that the limitation “domain name” in claims 1 and 26 is supported for the first time in US Application Ser. No. 09/504,783 (now U.S. Patent No. 6,502,135) a prior related application filed on February 15, 2000. *Id.* at 7; see Ex. 1050 (63). Petitioner cites numerous other proceedings where “Patent Owner has not disputed that claims reciting a ‘domain name’ are not entitled to an effective filing date prior to February 15, 2000.” Pet. 8. We find that the record supports that, for purposes of this case, the effective filing date of the ’705 patent is February 15, 2000, and the critical date for prior art under 35 U.S.C. 102 (b) is February 15, 1999.

¹⁹ Petitioner filed a Motion to Submit Supplemental Information pursuant to 37 C.F.R. § 42.123(a) asking that Exhibits 1057–1059 be considered as supplemental information, which we granted. See Papers 13–17.

Exhibits 1057–59 each relate to the Hopen Declaration. Petitioner contends they support a finding of the public availability of Aventail. Paper 14, 2, 5–8. Exhibit 1057 is a “redacted rough draft” of Mr. Hopen’s deposition from a related district court litigation, *VirnetX, Inc. v. Apple Inc.*, 10-cv-00417 (E.D. Tx.), which Patent Owner submitted to the Office as part of an Information Disclosure Statement (“IDS”) in the prosecution of U.S. App. No. 13/339,257. *Id.* at 6 n.3. Exhibit 1058 is a declaration of Mr. Hopen from a reexamination proceeding marked as deposition exhibit P4 at Mr. Hopen’s deposition. *Id.* Exhibit 1059 is jury trial transcript of another related district court case, including excerpts from Mr. Hopen’s deposition read into the record. *Id.* at 8; *see* Ex. 1059, 21–32.

Apart from whether they are admissible, Patent Owner argues the Hopen, Chester, and Fratto declarations do not prove Aventail was a printed publication publicly available as of January 31, 1999. PO Resp. 47–51. Further, Patent Owner contends the declarations are uncorroborated. *Id.* at 48 (citing *Typeright Keyboard Corp. v. Microsoft Corp.*, 374 F.3d 1151, 1158–60 (Fed. Cir. 2004); *Finnigan Corp. v. ITC*, 180 F.3d 1354, 366 (Fed. Cir. 1999)).

The testimony relates to the Exhibits regarding Aventail as prior art manuals: Aventail Connect v3.01/v2.51 Administrator’s Guide (Ex. 1009); Aventail Connect v3.01/v2.51 User’s Guide (1996–1999) (Exhibit 1010); and Aventail ExtraNet Center v3.0 Administrator’s Guide (Exhibit 1011). Patent Owner refers to Exhibit 1009 as corresponding to the testimony describing “Aventail Connect v3.01,” which Patent Owner, in turn, refers to in places as “Aventail.” *See, e.g.*, PO Resp. 50–51 (“Mr. Fratto’s testimony . . . stat[es] that he received a single copy of *Aventail*.” “[T]his statement by

Mr. Hopen cannot relate to Aventail Connect v3.01 and by extension *Aventail* because” “With regards to Aventail Connect v3.01 (the version of Aventail Connect corresponding to Ex. 1009), Mr. Chester’s testimony”).

Patent Owner acknowledges that Mr. Hopen states in his declaration that the AEC v3.0 product was distributed along with a copy of Aventail Connect v3.01/2.51 Administrator’s Guide (Ex. 1009) no later than January of 1999. *See* PO Resp. 48 (citing Ex. 1023 ¶¶ 13–15). Although Patent Owner also acknowledges the Hopen Declaration testimony that “‘thousands of copies of’ Aventail Connect v3.01 were distributed during the first six months of 1999,” Patent Owner contends “Mr. Hopen provides no evidence of how many copies were distributed in *January of 1999*—the date alleged by Petitioner as the latest publication date of *Aventail*.” *Id.* at 49 (citing Pet. 18; Ex. 1023 ¶¶ 9, 16). Patent Owner also argues the Fratto and Chester Declarations do not corroborate Mr. Hopen’s testimony that “‘thousands of’ copies of *Aventail* were distributed.” *Id.* at 50. Patent Owner contends that the declarations fail to show how much of the distribution occurred in January of 1999, the date alleged by Petitioner as the publication date of *Aventail*. *See id.* at 49–50.

Mr. Hopen testifies he was involved in the “design, development and distribution of all of Aventail’s network security products.” Ex. 1023 ¶ 4. Mr. Hopen also generally testifies that “Aventail included printed manuals with the software packages that it distributed.” *Id.* ¶ 8. Mr. Hopen testifies to an initial release of the “AEC” product as version 3.0, or AEC v3.0, which included version 3.01/2.51 of Aventail Connect and version 3.0 of the Aventail Extranet Server. *Id.* ¶ 13. He testifies that the AEC v3.0 product

included three software components. *Id.* ¶ 11. He testifies that Aventail announced a release of AEC in an October 12, 1998 press release. *Id.* ¶ 10 (attaching Ex. D to Ex. 1023). Aventail Connect v3.01/2.51 (i.e., Ex. 1009, Ex. E of Ex. 1023) and Aventail Extranet Center v3.01 Administrator’s Guide (i.e., Ex. 1011, Ex. F of Ex. 1023) was distributed with the software, and the software product was “publicly distributed . . . no later than January of 1999” (see *id.* ¶¶ 8, 14–16), with thousands of copies distributed “during the first six months of 1999” (*id.* ¶ 16).

We find that the testimony of Mr. Hopen shows that at least a portion of the thousands of copies of Exhibits 1009 and 10011 were distributed in January of 1999 through February 15, 1999. We also find that the October 8, 1998 press release (Ex. H of Ex. 1023) coupled with the testimony regarding actual distribution during January of 1999, shows that persons interested in the AEC software product including AEC v3.0, would have had access to its associated manuals (i.e., at least Exhibits 1009 and 1011) such that they were publically available prior to February 15, 1999.

Mr. Fratto is editor of the *Network Computing* magazine and website. Ex. 1043 ¶ 2. Mr. Fratto testifies that between 1997 and 1999 he reviewed and published articles on “Aventail Extranet Center (‘AEC’), which included client software called ‘Aventail Connect’ and server software called ‘Aventail Extranet Server.’” See *id.* ¶¶ 6–14 (citing articles attached to his declaration). Mr. Fratto also testifies that he received a copy of the “Aventail Connect v.3.01/2.51 Administrator’s Guide,” attached as Exhibit G to his declaration, which “was distributed with the AEC v3.0 product” in October of 1998. *Id.* ¶¶ 12, 14. A published article in October of 1998 corroborates his testimony about an announcement and release by Aventail

Corp. of the Aventail Extranet Center 3.0 product. *Id.* ¶ 13 (citing Exhibit I to his declaration, a “Network World” article).

Patent Owner contends that Mr. Fratto is biased against patents generally and Patent Owner specifically. PO Resp. 51 (citing Exs. 2023–35).²⁰ Our review of the cited Exhibits confirms that Mr. Fratto commented unfavorably about certain perceived patent types and his role as a witness. Nevertheless, Mr. Fratto’s statements in the cited Exhibits do not extend to all patents, all cases, and the patent system in general. Any bias Mr. Fratto may have against what he characterized as “stupid, obvious” patents, or similar characterizations that Patent Owner relies upon, in social media or otherwise, does not relate to his testimony at issue here, which pertains to the public dissemination issue. *See* PO Resp. 51 (citing Ex. 2034; Ex. 2036, 86:1–87:21).

Further, the record corroborates Mr. Fratto’s testimony. *See, e.g.*, Ex. 1043 ¶ 13 (citing Exhibit I attached to Exhibit 1043, “Intranet Applications: Briefs,” *Network World*, 55 (October 19, 1998)). Mr. Hopen’s testimony corroborates it further, because the testimony by each shows that the relevant software products were shipped with at least one of the manuals at issue here (i.e., Ex. 1009) before the end of January 1999. *See* Ex. 1023 ¶¶ 8, 14–16; Ex. 1043 ¶¶ 13–14 (Mr. Fratto received Exhibit G with the AEC v3.0 product). They also each testify about, and provide attached evidence of, published press release announcements of the AEC product in October of 1998. Ex. 1023 ¶ 10 (Ex. D, Oct. 12, 1998 press release

²⁰ By way of example, Patent Owner states “Mr. Fratto announced that he views his role as including ‘patent busting’ rather than ‘patent consulting.’” PO Resp. 51 (citing Ex. 2033; Ex. 2036, 94:4–11).

announcing “Aventail ExtraNet Center” software product); Ex. 1043 ¶ 13 (Ex. I, Oct. 19, 1998 *Network World* Brief announcing “the Aventail Extranet Center 3.0” software product release). Mr. Chester’s testimony, discussed further below, similarly corroborates Mr. Fratto, and “recall[s] that Aventail announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January 1999.” Ex. 1022 ¶ 15. Accordingly, we do not discount Mr. Fratto’s testimony. *See* Pet. Reply 17 n.4 (alleging the “attacks against Mr. Fratto are irrelevant and unfounded”).

Patent Owner also asserts that Mr. Fratto has a specific bias against Patent Owner because he has given testimony against Patent Owner’s patents and been compensated for it as an expert witness. *See* PO Resp. 51 (citing Ex. 2033; Ex. 2036, 49:17–50:9, 92:20–93:14). This alleged bias does not provide sufficient cause to diminish the weight given Mr. Fratto’s testimony. Carried to its logical extreme, expert testimony always could be diminished because it would always be “biased against” the opposing party.

Mr. Chester is CEO of Assured Products Group, a software development and consulting firm. Ex. 1022 ¶ 4. Mr. Chester worked for IBM between March 1992 and August 2002 evaluating network security products. *Id.* ¶ 5. Mr. Chester evaluated Aventail VPN products between 1996 and 2000. *Id.* ¶ 9. Mr. Chester “recall[s] that Aventail announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January 1999.” *Id.* ¶ 15. Mr. Chester testifies that the AECv3.0 product included version 3.01/2.51 of the Aventail Connect software and version 3.0 of the Aventail Extranet Server. *Id.* ¶ 16. He testifies that he received “Exhibit C with the AEC v3.0 product” “no later than July 1998” and “Exhibit C is a copy of the Administrator’s Guide for

Aventail Connect v.3,01/2.51”—i.e., Exhibit 1009. Ex. 1022 ¶¶ 16–17, pp. 97–98 (Exhibit C to the Chester Declaration, which corresponds to Exhibit 1009).

Neither Mr. Hopen, Mr. Fratto, nor Mr. Chester have been shown to have any relationship or interest in the outcome of this proceeding. There is no evidence or even argument that Aventail Corporation, for whom Mr. Hopen worked, is a competitor to Patent Owner. Although both Mr. Fratto and Mr. Chester received compensation for their testimony, expert witnesses typically receive compensation, and nothing in the record indicates bias based on compensation. *See, e.g.*, Ex. 1022 ¶ 2; Ex. 1043 ¶ 5.

Although the testimony of the three witnesses is sufficient to establish the Aventail documentation is prior art, Petitioner offers additional evidence of corroboration submitted with the declarations, which Petitioner argues Patent Owner ignores. Pet. Reply 17 (citing Ex. 1023, 7 (announcement), 10 (article), 94 (announcement), 293 (announcement), 295 (press release), 424 (article)). The cited exhibits do not relate directly to the Aventail client software or Aventail manuals, but constitute evidence that the Aventail Corporation was developing VPN security products in mid-1997 and late 1998. *See* Ex. 1023, 9 (“For secure remote-access needs, Aventail Corporation’s Mobile VPN 2.0 and AutoSocks 2.1 comprise a virtual private network (VPN) software solution . . .”). This evidence ties into the timeline of Aventail Corporation’s VPN products introduced between 1996 and 2000, as Mr. Chester describes. *See* Ex. 1022 ¶¶ 9–13. Petitioner cites additional evidence, also related to Aventail Corporation products. *See* Pet. Reply 17 (citing Ex. 1057, 79:25–80:9, 83:10–84:16, 91:20–92:2, 100:2–104:7; Ex. 1059, 20–32).

The testimony at pages 100–104 of Mr. Hopen’s deposition (Exhibit 1057) describes Exhibit 9 of his deposition, Aventail Connect version 3.01/2.51 Administrator’s Guide (Ex. 1009 here), and correlates it with a discussion about an October 1998 date of a press release for the Extranet Center 3.0 product. See Ex. 1057, 100:2–104:4. The Hopen deposition testimony was taken in the district court litigation and was subject to cross-examination by Patent Owner. See Ex. 1057, 148:1–227:4 (examination by Patent Owner’s attorney Mr. Curry). The cross-examination, and the fact that the testimony is consistent with Mr. Hopen’s declaration, adds to the credibility of Mr. Hopen’s testimony.

Even if corroboration is somehow required to show public availability, corroboration “does not require that every detail of the testimony be independently and conclusively supported by explicit disclosures in the pre-critical date documents or physical exhibits.” *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1348 (Fed. Cir. 2013). *Willow Wood* stated a “rule of reason” test in which “the totality of the evidence . . . including circumstantial evidence” is assessed “in order to ascertain whether the testimonial assertions are credible.” *Id.* “A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

The evidence as outlined above supports a finding that persons interested and ordinarily skilled in the subject matter of the manuals could

have located them. The evidence shows that Aventail Corp. announced release of the products and they were disseminated with the manuals. In addition, two declarants had actual access to the Aventail Extranet Center v3.0 product, and its manuals, by January 1999. In the case of Mr. Fratto, as indicated above, between 1997 and 1999, he reviewed and published articles for his *Network Computing* magazine and website relating to “Aventail Connect” and “Aventail Extranet Center.” Ex. 1043 ¶¶ 2, 6. As also noted above, Mr. Fratto testified that the Aventail Extranet Center 3.0 product was distributed in the fall of 1998 and identified “Intranet Applications: Briefs,” *Network World*, 55 (October 19, 1998) (Exhibit I to Ex. 1043) as support. *Id.* ¶ 13. Mr. Fratto identified Exhibit G as a non-confidential copy of Aventail Extranet Center v3.0 (Ex. 1009) he received in October 1998. *Id.* ¶ 14. Mr. Chester testifies generally that, while at IBM, “the Aventail products were distributed with installation disks and printed manuals.” Ex. 1022 ¶ 12. He specifically testifies about a press announcement about Aventail Corp. releasing the AEC v3.0 product, testifies about receiving the Administrator’s Guide for Aventail Connect v3.0/2.51 (Exhibit C to the declaration, Ex. 1009 here), “no later than July 1998,” and testifies that Aventail Corp. “began distributing this product no later than mid-January of 1999,” which he knew about because “he was personally involved” at IBM with Aventail. *Id.* ¶¶ 15–17.

After listing Exhibits 1009–11, Dr. Tamassia states that the Aventail “documents cross-reference each other, which is logical as they are describing two components of a single system that are designed to work together (i.e., the Aventail Connect client running on the client computer, and the Aventail Extranet Server running on a server computer).” *See* Ex.

1005 ¶ 182 (listing documents), ¶ 183 (citing Ex. 1009, 3, 5, 6, 11, 14, 19, 36–40, 44, 46, 48, 50, 52, 55–57, 61–71, 76, 77, 79–83, 92–94, 96, 99, and 107–109). As one cited example, Aventail (Ex. 1009, 14) refers to a CD that “contains the Administrator’s Guide and the User’s Guide” for help in executing Aventail Connect —i.e., the latter reasonably pointing to the availability of Exhibit 1010 (“Aventail Connect v3.01/v2.51 User’s Guide (1996–1999)”). Exhibit 1009 also states that “[f]or additional information on how to configure the Aventail ExtraNet Server product, consult the Aventail ExtraNet Server Administrator’s Guide [i.e., Ex. 1011].” Ex. 1009, 73.

Therefore, the record supports the unchallenged evidence of cross-referencing as to the inter-related products (Aventail Connect and the SOCKS server, ExtraNet, etc.) and the three manuals at issue, thereby supporting the finding that because at least Exhibits 1009 and 1011 were accessible and disseminated as discussed above, Exhibit 1010 also would have been accessible to persons interested in the subject matter of the Aventail v3.0 product. Furthermore, skilled artisans seeking Aventail v3.0 products would have sought out relevant and existing documentation for using and/or acquiring the product. The record evidence shows that the testimony of Mr. Hopen, Mr. Fratto, and Mr. Chester is credible, and supports Petitioner’s showing by a preponderance of the evidence that Exhibits 1009–11 of Aventail not only were publically available, but Exhibits 1009 and 1011 also were disseminated to persons of ordinary skill interested in computer networking and security as of January 1999.

Viewing the evidence as a whole, Petitioner has shown persuasively that Aventail was publicly available before February 15, 1999. Accordingly,

we find that Petitioner has established, by a preponderance of the evidence, that the Aventail manuals, including Exhibits 1009–11 qualify as prior art printed publications under 35 U.S.C. § 102(b).

2. RFC 2401 and RFC 2453

In our Decision to Institute, in addition to citing the Tamassia Declaration, we found that RFC 2401 and RFC 2543 each independently include indicia suggesting a reasonable likelihood that the documents were publically available:

RFC 2401 and RFC 2543 each include dates on each page, and the cover sheets bear the designations “Request for Comments” from the “Network Working Group,” discussing particular standardized security protocols for the Internet. Ex. 1008, 1; Ex. 1013, 1. Each document describes itself as a “document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements Distribution of this memo is unlimited.” Inst. Dec. 9 (citing Ex. 1008, 1; Ex. 1013, 1; Ex. 1005 ¶¶ 186–97 (discussing Request for Comment (“RFC”) publications)).

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.* ¶¶ 186–193 (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.* ¶ 190 (citing Ex. 1036, 20). Dr. Tamassia quotes RFC 2026, which explains that anyone can obtain RFCs from “a number of Internet hosts,” making the

“working document readily available to a wide audience, facilitating the process of review and revision.” Ex. 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. 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. 54.²¹ Patent Owner also contends that nothing shows that interested persons could have located the documents. *See* PO Resp. 54–56.

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.²² The contents of RFC 2401 and 2543 are consistent with the publication

²¹ 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.6. Patent Owner, itself, however, directed the Board’s attention to this testimony in its Preliminary Response. Paper 6, 5–6. Therefore, Patent Owner had adequate notice of its contents to respond to it without resulting prejudice.

²² 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.

process described by RFC 2026 and Dr. Tamassia, including the requests for discussion and suggestions for improvements in each document, and the dates “November 1998” and “March 1999” respectively on the top right corner of the first page of each document. *See* Ex. 1008, 1; Ex. 1013, 1.²³ The title itself on each document, “Request for Comments,” coupled with evidence in RFC 2026 that each RFC document was made widely available “from a number of Internet hosts,” constitutes sufficient evidence that RFC 2401 and 2543 each was intended for publication and would have been accessible to interested artisans seeking documents related to “Internet standards.” Ex. 1036, 6, 8, Ex. 1008, 1; Ex. 1013, 1; Ex. 1005 ¶¶ 187–89. In other words, these documents—each a request for suggestions and improvements for Internet standards and having no indication of being a mere draft or internal paper—are precisely the type of documents whose main purpose is for public disclosure. The Tamassia Declaration specifically references RFC 2401 and RFC 2543, including their publication dates. *See, e.g.*, Ex. 1005 ¶¶ 194–197.

“A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l*, 511 F.3d at 1194 (quoting *Bruckelmyer*, 445 F.3d at 1378). Faced with record evidence as set forth in the Institution Decision, as part of routine discovery, *see* 37 C.F.R. § 42.51(b)(1)(ii), Patent Owner had the opportunity

²³ The March 1999 date renders RFC 2543 prior art under 35 U.S.C. § 102(a). *See* Ex. 1005 ¶ 197 (acknowledging same).

to cross-examine Dr. Tamassia about the RFC documents and process of publication, but does not point us to any discussion of the issue.

We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401(dated November 1998) and RFC 2543 (dated March 1999) were made available to persons of ordinary skill interested in computer networking and security sufficiently to be deemed “publicly accessible” at the relevant time. *See SRI Int’l*, 511 F.3d at 1194. Therefore, we determine RFC 2401 and RFC 2543 qualify as prior art printed publications respectively under 35 U.S.C. § 102(b) and 35 U.S.C. § 102(a).

3. Overview of Aventail

Aventail Connect represents the client component of the Aventail ExtraNet Center. *See* Ex. 1009, 7. Aventail Connect automatically routes traffic from WinSock to the Aventail ExtraNet Server, which is an extranet (SOCKS) server, in order to allow the workstations to use the SOCKS v5 protocol—an Internet Engineering Task Force approved security protocol for securely traversing corporate firewalls. *Id.* at 6–7. In other words, Aventail Connect can be used in a network as a simple proxy client for managed outbound access and secure inbound access. *Id.* at 7. In addition, “Aventail Connect can establish an encrypted tunnel automatically.” *Id.* Aventail Connect also can compress or encrypt data before routing to the network. *Id.* “[B]ased on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.” Ex. 1009, 73.

Aventail Connect can compress or encrypt data before routing to the network. *Id.* at 9. The routing is determined by rules described in the configuration file. *Id.* When Aventail Connect receives a connection

request, it determines whether or not the connection needs to be redirected to an Aventail ExtraNet Server and whether the connection should be encrypted. *Id.* at 10. This process is described using several steps. *Id.* at 11–13.

In the first step, Aventail Connect performs a DNS lookup to convert the hostname to an IP address. Ex. 1009, 11. If the application knows the domain is one to which traffic is being proxied (i.e., the destination hostname matches a redirection rule domain name from the configuration file), a false DNS is created that later can be recognized during a connection request. *Id.* Similarly, if a DNS proxy option is enabled, but the domain cannot be looked up directly, the application again creates a false DNS entry that it can recognize later, and returns this to the calling application. *Id.* at 12. The false entry tells Aventail Connect that the DNS lookup must be proxied (forwarded to and resolved by an extranet server) in the next step of the process. *Id.* Otherwise (if Aventail Connect already knows the IP address of the hostname, the hostname matches a local domain string, or the hostname does not match a redirection rule, and no proxy option is enabled), the DNS lookup proceeds as if Aventail Connect were not running. *Id.*

In the second step, Aventail Connect requests a connection to the remote host. Ex. 1009, 12. The request is first checked to see if it contains a false DNS entry, as may be assigned set in the first step. *Id.* If a false DNS entry is present, the request is proxied—sent to an extranet server (“SOCKS”) for hostname resolution using the authentication method specified in the configuration file. *Id.*

Once the connection is complete, in the third step, Aventail Connect transmits and receives data. *Id.* at 12. This data may be encrypted for

transmission and decrypted on receipt if “an encryption module is enabled and selected by the SOCKS server.” *Id.*

“Only traffic destined for the internal network [behind the Aventail ExtraNet Server in the VPN] is authenticated and encrypted; all other traffic passes through Aventail Connect unchanged.” *Id.* at 73. “[N]o direct network connections between the public LAN and the private LAN can be created without being securely proxied through the Aventail ExtraNet Server.” *Id.* at 72. Client work stations must have Aventail Connect to connect to the extranet:

Due to the routing restrictions described above, these clients will have no network access beyond the Aventail ExtraNet Server unless they are running Aventail Connect. Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.

Id. at 72–73.

In summary, when a calling application, for example, an e-mail application or a browser, requests to communicate with an external network destination, Aventail Connect intercepts it. *See* Ex. 1009, 8, 11. If the destination matches a redirection rule domain name or a proxy option is enabled, Aventail Connect creates a false DNS that later will be recognized during a connection request as one to be proxied to the Aventail ExtraNet Server. *See id.* at 10–12. “When the Aventail Connect . . . receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted” *Id.* at 10.

4. Overview of RFC 2401

RFC 2401 describes security services offered by the IPsec protocols, including “access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption).” Ex. 1008, 3–4. 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.*

5. RFC 2543

RFC 2543 describes a network-based secure video telephony architecture that supports both audio and video (i.e., multimedia). Ex. 1013, 1, 137. These multimedia telephony sessions may use end-to-end encryption. Ex. 1013, 54.

6. Obviousness Grounds Based on Aventail, RFC 2401, and RFC 2543

Petitioner alleges claims 1–23 and 25–30 would have been obvious over Aventail, RFC 2401, and RFC 2543. *See* Pet. 17–30 (summarizing prior art), 30–58 (addressing claim limitations).

i. Claims 1 and 16—Determination and Request

Claim 1 of the ’705 patent recites a “determination as a result of the request that the target device is a device with which a secure communication

link can be established.” The “request,” generated by the client device, constitutes a “request . . . to look up an internet protocol (IP) address of the target device based on a domain name associated with the target device.”

Claim 16 recites similar limitations.

Petitioner sets forth the following description of Aventail relevant to the determination and request clauses: In one configuration, a redirection configuration, Aventail Connect consults a table of redirection results to determine if the target hostname (a domain name) corresponds to a host device known to be available via an Aventail ExtraNet Server. *See* Pet. 22 (citing Ex. 1009, 8–12), 36. If so, then “Aventail Connect proxies that request to the Extranet server.” *Id.* at 22 (citing Ex. 1009, 11–12). In another configuration, a proxy configuration, the system simply proxies the request to the ExtraNet Server (rather than evaluating it on the client), which resolves the target host name. *Id.* (citing Ex. 1009, 12, 61; Ex. 1005 ¶¶ 263–266).

Under either configuration, “if a request contains a domain name to be proxied to the Extranet server,” Aventail Connect flags the request by inserting a “false” DNS entry called a “HOSTENT,” as the network address, “into the response to the request to lookup the domain name.” Pet. 23 (citing Ex. 1009, 11–12; Ex. 1005 ¶ 275). “Once the DNS query has been resolved,” the requesting client then uses that “resolved” false entry (instead of a resolved network address) for a connection request, Aventail Connect recognizes the request as one to be proxied, and “Aventail Connect will proxy the connection request to the Extranet server.” *See id.* at 22–23 (citing Ex. 1009, 12; Ex. 1005 ¶¶ 276–277). In proxying the connection request, Aventail Connect recognizes the “HOSTENT” false entry and

inserts a “fully qualified hostname” to the ExtraNet server for the “proxy” resolution. Ex. 1009, 11–12.

According to Dr. Tamassia,

Aventail explains that if the domain name in a request does not match a local domain string (or if there are no local domains stored at the client), the domain name value in the request will then be compared against a second table of values, called redirection rules, unless the “DNS proxy option” is enabled.

Ex. 1005 ¶ 263 (citing Ex. 1009, 11–12); *see also id.* ¶ 265.

According to Petitioner, “for these connections, Aventail Connect can be configured to establish an encrypted and authenticated connection that enables the application to securely communicate with the remote host.” Pet. 23 (citing Ex. 1009, 12; Ex. 1005 ¶¶ 276–292, 293–294); *see* Ex. 1005 ¶ 256 (flowchart).

With respect to the intercept clause, Petitioner contends that Aventail discloses it “in two ways.” Pet. 36. First Aventail Connect intercepts a request from the client that includes a domain name. Pet. 36–37 (citing Ex. 1009, 7–9, 72–73, 90–92; Ex. 1005 ¶¶ 209, 210, 247–54, 266); *see also* Pet. 39 (citing Ex. 1009, 11–12; Ex. 1005 ¶¶ 267–75). Second, the Aventail ExtraNet server will resolve a hostname (provide a look up) for access to private secure devices in a proxy request. Pet. 37–38 (citing Ex. 1009, 12; 61; Ex. 1005 ¶¶ 263–266); Ex. 1005 ¶ 264 (“the proxy server will be responsible for resolving the DNS lookup request”). Summarizing, “either the client computer running Aventail Connect or the Extranet server receives and acts on the DNS requests – neither is the destination specified in the lookup request.” Pet. 38 (citing Ex. 1009, 12; Ex. 1005 ¶ 266).

Turning to the determination clause, Petitioner contends that Aventail discloses that Aventail Connect determines whether to redirect and encrypt

the connection based on a domain name in a request. Pet. 39 (citing Ex. 1009, 10). As support, Petitioner quotes the following statement in Aventail: “When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) **and/or encrypted** (in SSL).” Pet. 39 (quoting Ex. 1009, 10) (emphasis by Petitioner).

Petitioner explains further:

Inclusion of the remote host in the redirection rule table therefore enables Aventail Connect to determine if the remote host will require an encrypted connection (“*is a device with which a secure communication link can be established*”). Ex. 1009 at 8–9, 11–12, 40; *see also* Ex. 1005 ¶ 275. Aventail’s disclosure of using a lookup table to check whether a host is one requiring communications to be proxied is very similar to the technique disclosed in the ’0705 patent for determining availability of a host for a secure communications service. *See* Ex. 1050 at 40:6–13, 40:57–63.

Pet. 39–40.

Petitioner also relies on a “determination by the Extranet server” to “determine whether the client device is allowed (or denied) access to the target device.” *Id.* at 40. Petitioner quotes from the Aventail ExtraNet Admin. Guide (Ex. 1011) to support this position: “[T]he Extranet Server ‘determine[s] which people and groups can access what machines and services based on where they came from, the time of day, how they authenticated, and encryption strength, etc.’” *Id.* at 41 (quoting Ex. 1011, 19).

Relying on the known SOCKS standards and disclosure of SOCKS in Aventail, Petitioner also explains that “[a] person of ordinary skill would thus have understood this SOCKS-negotiation disclosure in Aventail to be

explaining the Extranet server would determine whether the client device is allowed (or denied) access to the target device to which the client device has requested a connection (also ‘*a determination*’).” *Id.* at 40 (citing Ex. 1009, 5, 12; Ex. 1005 ¶ 281; Ex. 1018, 5–6 (describing SOCKS negotiation procedures)).

Further regarding encryption as part of the determination, Petitioner explains that Aventail discloses a configuration whereby *all connections can encrypted*. “Aventail Connect flags the request to be proxied to the Aventail Extranet Server for handling, including establishing an encrypted connection *when Aventail Connect is configured to encrypt all communications*.” Pet. 39 (emphasis added) (citing Ex. 1009, 11–12, 73; Ex. 1005 ¶¶ 267–275). At one of the cited pages, Aventail describes encryption and authentication for “all users” attempting to connect to internal private networks via the Aventail ExtraNet Server:

User authentication and encryption on the Aventail ExtraNet Server require *all users to use Aventail Connect to authenticate and encrypt their sessions before any connection to the internal private network(s)*. For this example, the Aventail ExtraNet Server *encrypts all sessions with SSL*.

Ex. 1009, 73 (emphasis added).

Aventail discloses tailoring the “security policy” and “forward[ing] traffic” to private destinations internal to the Aventail ExtraNet Server:

Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.

Ex. 1009, 72–73.

In response, Patent Owner argues that Aventail does not disclose the determination step. PO Resp. 29–35. As indicated, claim 1 recites “a determination as a result of the request that the target device is a device with which a secure communication link can be established.” Patent Owner contends that the determination step must determine if the second device, the remote host in Aventail, “will require an encrypted connection,” arguing that security requires encryption. *See* PO Resp. 31. Patent Owner similarly contends that “[t]he redirection rules do not . . . imply that the remote host will require an encrypted connection because . . . *Aventail* does not teach an encrypted connection to the remote host.” *Id.* at 32 (citing Ex. 2018 ¶ 47). Patent Owner similarly contends that “requiring a proxied connection is not the same as requiring an encrypted connection.” *Id.* (citing Ex. 2018 ¶ 48).

Patent Owner also argues that even if the combination of Aventail and RFC 2401 “included an end-to-end encrypted channel,” Petitioner fails to explain how the redirection table “includes a ‘determination’ regarding encryption being required by a remote host.” *Id.* at 33. Patent Owner maintains that “at best Aventail’s disclosed system only determines whether to encrypt traffic to the SOCKS server but not to the remote host.” *Id.* (citing Ex. 1009, 12, step 3; Ex. 2018 ¶ 49). Patent Owner also contends that Petition relies on “the matching of a *domain name* against a redirection rule table” to reach the determination step, which Patent Owner contends occurs in step 1b of Aventail, but the Institution Decision incorrectly relies on a determination implied by a “connection request,” that includes determining “[w]hen redirection and encryption are not necessary,” which

“connection request” Patent Owner contends occurs in step 2 of Aventail. *Id.* at 34 (citing Inst. Dec. 15; Ex. 1009, 11–12; Ex. 2019, 191:11–24).

Patent Owner’s arguments are not persuasive. Petitioner shows that Aventail discloses determining if encryption should apply *for each connection*, including connections suggested by RFC 2401 as requiring end-to-end encryption. *See, e.g.*, Pet. 39; Pet. Reply 6–8. Patent Owner’s arguments rely on a separate attack of Aventail: Aventail does not disclose end-to-end encryption; therefore, Aventail does not disclose determining if there is end-to-end encryption. These arguments fail for two reasons. First, security does not require “end-to-end” encryption under our claim construction and it also violates the holding in *Cisco*, 767 F.3d at 1321 (VirnetX presented evidence that “the virtual private network extend[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”).²⁴ As in *Cisco*, the Aventail ExtraNet Server provides security behind that server in the corporate private network. *See, e.g.*, Ex. 1009, 73 (“Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server.”).

Second, even if security requires end-to-end encryption, as discussed above, and according to Petitioner’s challenge, Aventail discloses an option for encrypting all connections (at least up to the Aventail ExtraNet Server), and even if that disclosure does not include end-to-end encryption (behind

²⁴ *See also, 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’” (emphasis omitted)). Patent Owner does not argue that security requires encryption.

the server), the combination of Aventail and RFC 2401 suggests end-to-end encryption. Therefore, determining to proxy the connection to the Aventail ExtraNet Server constitutes a determination that the target device is available for a secure connection and requires encryption—either because all the devices require encryption or because the Aventail ExtraNet Server can decide to allow or deny the connection based on encryption strength (and authentication). *See* Ex. 1009, 73 (deny or allow based on security policy or require all users to encrypt “before any connection to the internal private network(s)”; Ex. 1011, 19 (administrator defines “rules for specifying which people and groups can access what machines and services. Rule elements include: where they came from, the time of day, how they authenticated, and encryption strength, etc.”).

Patent Owner’s other argument listed above asserting that Aventail does not disclose determining whether to apply encryption during step 1 in Aventail fails to outline why it matters in terms of any claim limitations.²⁵ Assuming for the sake of argument that Aventail only refers to a “connection request” in step 2, and not more broadly, as Petitioner replies, the challenged claims do not preclude that scenario. *See* Pet. Reply 7.

That is, as Patent Owner contends with respect to one disclosure, in step 2, “Aventail Connect checks the connection request” and if “the request contains a false DNS entry (from step 1), it will be proxied.” Ex. 1009, 12. Nevertheless, “check[ing] the connection request” in step 2 constitutes

²⁵ Also, contrary to Patent Owner’s arguments, the Petition does not rely solely Aventail’s step 1 as disclosing an interception of a request to look up a DNS in step 1 of Aventail—it also relies on a DNS look up at the Aventail ExtraNet Server, which resolves the fully qualified hostname during the proxy request.

determining if a target host “is a device with which a secure communication link can be established,” as claim 1 requires, according to Petitioner’s challenge and showing: “Inclusion of the remote host in the redirection rule table therefore *enables* Aventail Connect to determine if the remote host will require an encrypted connection (*‘is a device with which a secure communication link can be established’*).” Pet. 39–40 (citing Ex. 1009, 8–9, 11–12, 40) (emphasis added).

In other words, one of Petitioner’s theories includes determining in step 2 if the proxy contains a false DNS entry, based on the previous DNS request in Aventail’s step 1. And the determination step of claim 1 does not require the two steps that Aventail discloses to occur as one step—claim 1 implies separate steps. Claim 1 also does not require the determination to be based on an *intercepted* request or based on a *completed* look up of a domain name, it only must be based on the antecedent “*request . . . to look up . . . based on a domain name.*” Patent Owner’s arguments fail to upset Petitioner’s showing, and fail to articulate how its argument about steps 1 and 2 of Aventail matter.

In any case, even if the claim 1 determination step requires the determination to be based on an intercepted result and a resolved domain name, Petitioner’s showing as described above and herein also persuasively addresses it.

The passage at issue states the following:

When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack.

Ex. 1009, 10.

This passage, and other passages and evidence cited by Petitioner as discussed above, generally relate to a proxy situation involving the Aventail ExtraNet Server. In other words, Aventail Connect determines if “redirection and encryption are . . . necessary” (which may occur in step 2 of Aventail as Patent Owner argues) because Aventail Connect recognizes a proxy situation exists, and recognizes it based on a previously intercepted request for a DNS look up.

It also signifies that Aventail Connect recognizes configurations in which all proxied connections must be encrypted, as discussed above, and as Petitioner argues. *See* Pet. 39. Furthermore, the Aventail ExtraNet Server itself also satisfies the determination step, because it decides if it will provide a connection to a specified secure device and the level of encryption, as Petitioner also argues as summarized above, and as discussed further below. *See* Pet. 41; Ex. 1009, 72–73 (“based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed”).

In other words, contrary to Patent Owner’s arguments and to the extent the claims require a determination in response to a look up, Aventail discloses ultimately that as a response to a domain name look up request, the system determines if encryption applies and if a client can access a relatively secure (i.e., private) host behind the ExtraNet Server. If the proxy configuration or the redirection rules apply, a request includes a “fully qualified hostname” (Ex. 1009, 12), which Aventail Connect “forward[s]” (*id.* at 11) to the Aventail ExtraNet Server, which then responds by determining, in conjunction with a SOCKS negotiation, whether to allow or

deny the connection. *See* Pet. 40 (citing Ex. 1009, 5, 12; Ex. 1005 ¶¶ 280–81); Ex. 1009, 11–12, 72–73. Therefore, the Aventail ExtraNet Server with a SOCKS negotiation determines based on the requested target host name that the client can connect to a specified secure target device in the VPN behind the Aventail ExtraNet Server and whether the connection supports encryption. *See* Ex. 1009, 10–12, 72–73; Ex. 1005 ¶¶ 203–06, 280–84.

Aventail Connect also provides the capability to determine whether the connection should be encrypted by determining if proxy applies, with Aventail Connect and Aventail ExtraNet Server additionally interacting to establish the encrypted channel and determine what machine and level of security applies. *See* Ex. 1009, 11–12, 72–73; Ex. 1005 ¶¶ 279–280 (citing Ex. 1009, 10, 12).

As indicated above, the determination limitation recites a determination that the second network device is available for a secure communications service. Petitioner contends that even if Aventail does not explicitly disclose end-to-end encryption (as a form of security) to the target hosts, RFC 2401 suggests the limitation in Aventail’s similar system—i.e., “end-to-end encryption, including one which provides this over firewall or proxy computers that sit between the originating and destinations of the end-to-end communication path.” Pet. 44; *see also* Pet. 28–29 (citing Ex. 1008, 25–26), 43–44 (citing “Case 4”; Ex. 1005 ¶¶ 403–20).

Petitioner provides several reasons supported by the record as to why end-to-end encryption would have been obvious, including the “similar schemes” (i.e., comparing RFC 2401 Case 4 and the Aventail ExtraNet Server to suggest encryption through firewalls or proxies), to ensure security over the entire path via encryption in order “to increase security in certain

scenarios, such as when a remote client connect[s] to a server with sensitive information,” and “sending IPSec encrypted network traffic through proxy or firewall computers without being decrypted” (i.e., instead of the Aventail ExtraNet Server doing the decrypting for many devices). See Pet. 44–45 (citing 1005 ¶¶ 403–420; Ex. 1008, 3–4; Ex. 1009, 7, 11–12, 72–73; Ex. 1020, 5:46–49, 17:47–51 (suggesting end-to-end encryption to enhance security for highly sensitive information in private networks); Ex. 1021, 1:25–27 (internal encryption for ensuring security of an organization’s sensitive information)).

In general, the Aventail system provides security from client to target devices in a private network connected to and beyond the Aventail ExtraNet Server and satisfies the determination step in several ways as Petitioner contends: “[B]ased on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.” Ex. 1009, 73. Also, “[w]hen the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL).” *Id.* at 10; see also Ex. 1009, 73 (“Only traffic destined for the internal network is authenticated and encrypted; all other traffic passes through Aventail Connect unchanged.”). Dr. Tamassia testifies that

if Aventail Connect determines that the hostname in the intercepted DNS request matches one of the destinations for which a redirection rule has been defined, then Aventail Connect will evaluate the redirection rule to determine if the target host is one for which proxy redirection (and an encrypted communication) through the Aventail ExtraNet Server is required.

Ex. 1005 ¶ 275 (citing Ex. 1009, 11). Petitioner also relies on Aventail’s disclosure that the ExtraNet Server “determine[s] which people and groups can access what machines and services based on where they came from, *the time of day, how they authenticated, and encryption strength, etc.*” Pet. 40 (quoting Ex. 1011, 19) (emphasis added).

The record supports Petitioner. As Petitioner contends, Patent Owner and Dr. Monroe do not address the Petition’s reliance on the Aventail disclosure in Extranet Center Admin. Guide (Ex. 1011) (referenced at Aventail, Ex. 1009, 73) that describes the ExtraNet Server focusing on “what machines and services” behind the ExtraNet server can be accessed, based in part on the requester’s authentication and encryption strength. See Pet. Reply 8–9; Ex. 1011, 19. Patent Owner’s related argument that the determination clause precludes gauging a user’s relative authentication and encryption strength to determine if the “target device is a device with which a secure communication link can be established” is not persuasive. See PO Resp. 34–35 (emphasis omitted). As Petitioner contends, the ’705 patent contemplates matching security levels and using authentication—so that part of the determination in Aventail and in the ’705 patent may include determining whether the target device is available *to a specific user*. See Pet. Reply 8 (citing Ex. 1050, 40:57–59).

Finally, Aventail discloses encryption and decryption by Aventail Connect, but this panel is unable to find a disclosure in Aventail of a decryption feature at the ExtraNet Server. See Ex. 1009, 1 (“Aventail Connect is a proxy client, but when used with SSL it provides the ability to encrypt inbound and outbound information.”). This, and other disclosures discussed above, supports Petitioner’s obviousness analysis based on the

suggestion in RFC 2401 to provide encryption beyond a firewall or proxy server such as the ExtraNet Server to ensure end-to-end security, and a corresponding determination that target hosts match a desired level of encryption determined by the ExtraNet Server. *See* Ex. 1009, 12, 59–67, 72; Ex. 1008, 3–4, 24–26; Pet. 45–46; Ex. 1005 ¶¶ 412–415, 420. Accordingly, the record shows that Aventail discloses encrypting select traffic at least up to the Aventail ExtraNet Server based on matching the client to host target security resources, which specifies a certain matched security, including encryption. RFC 2401 discloses encrypting traffic beyond a firewall or gateway server to provide added security to the communication, thereby further suggesting, in combination with Aventail, a determination of security, and under Patent Owner’s claim construction, determining if a target host accepts encryption.

Consequently, Petitioner has provided an articulated reasoning with some rational underpinning to support the legal conclusion of obviousness as to the determination and request limitations. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

*ii. Claims 1, 6, 16, and 22—Direct Connection—
Secure Communication Link, VPN Link*

Patent Owner contends that Aventail does not disclose “a secure communication link” because Aventail does not disclose a direct Connection. PO Resp. 36. Patent Owner also contends that the combination of Aventail and RFC 2401 would not result in a direct connection because “the connection would still be relayed through the intermediate SOCKS server which would cause the resulting combination to not have a direct

encrypted connection with a remote host.” *Id.* at 36–37 (citing Ex. 2018 ¶¶ 54–55).

Patent Owner’s arguments are not persuasive, because they rely on a claim construction that we do not adopt. A secure communication link and VPN link do not require a direct link.

Even if they do, Petitioner contends that “Aventail expressly teaches that ExtraNet Servers are capable of ‘directly’ forwarding encrypted network traffic.” Pet. 46 (quoting Ex. 1009, 63; Ex. 1005 ¶¶ 417–20). Aventail supports Petitioner: “Depending on the security policy and the Aventail ExtraNet Server configuration, *Aventail Connect will automatically proxy their allowed application traffic into the private network.*” Ex. 1009, 72–73 (emphasis added). That is, traffic goes *into the private network* through the Aventail ExtraNet Server. In preceding paragraph, Aventail states that “no *direct* network connections between the public LAN and the private LAN can be created *without being securely proxied through the Aventail ExtraNet Server.*” Ex. 1009, 72 (emphases added). These statements show further that the Aventail ExtraNet Server creates a direct, secure connection, in a secure communication link or VPN link, to target hosts in a private LAN.

Dr. Tamassia explains that the SOCKS (Aventail ExtraNet) server as disclosed in Aventail can be a firewall, or behind the firewall as a dedicated server, similar to a gateway to a private network. See Ex. 1005 ¶¶ 200, 226. *Cisco*, 767 F.3d at 1320, indicates that a direct connection does not preclude such a forwarding server or similar corporate gateway device.

As Petitioner persuasively contends:

[N]either Patent Owner nor its expert have attempted to explain what is required by “direct[ness].” Resp. at 8–13, 36–38. To the extent the term itself is informative, Aventail describes the

“network connections” that are proxied between client computers and those on the private network as “direct network connections.” Ex. 1009 at 72 (“[N]o **direct network connections** between the public LAN and the private LAN can be created **without being securely proxied** through the Aventail ExtraNet Server.”).

Pet. Reply 9–10 (emphases by Petitioner).

Patent Owner relies on Dr. Monroe, and contends that a proxy connection, such as via the SOCKS server, is not direct, because “Aventail discloses that the connection is terminated at the SOCKS server.” PO Resp. 37. Patent Owner also contends that because “Aventail Connect encrypts the data on its way to the server,” this also shows that the connection is not direct. *See id.* Patent Owner also contends that “the operation of *Aventail*, as discussed above, is different from a regular firewall or an edge router or gateway, where the traffic is destined for the target device and not for the firewall or the edge router or the gateway.” *Id.* (citing Ex. 2018 ¶ 55).

Patent Owner contends that the statement in Aventail that “no direct network connections between the public LAN and the private LAN can be created without being securely proxied through the Aventail ExtraNet Server,” actually means the opposite of what it says, contending that it means “that a direct connection between the public and private LANs is not possible because the connection has to be proxied through the SOCKS server.” *Id.* at 38 (citing Ex. 2018 ¶ 56). Dr. Monroe testifies similarly. *See* Ex. 2018 ¶ 56. Contrary to Patent Owner’s argument, the statements on pages 72–73 of Aventail contradict the testimony of Dr. Monroe and Patent Owner’s assertions. Ex. 1009, 72. Moreover, in *Cisco*, the court affirmed a finding of infringement even though the infringing system included

intermediate “VPN servers, VPN authentication servers, proxy servers, and firewalls.” *Cisco*, 767 F.3d at 1322.

Furthermore, Patent Owner’s citations to Aventail do not support the argument that the Aventail ExtraNet Server terminates a connection (assuming for the sake of argument that “direct” implies such a non-termination feature). Patent Owner’s arguments also imply that “direct” means that traffic “is destined for the target device and not for the firewall or the edge router.” PO Resp. 33. Patent Owner does not provide any interpretation of what direct means in its claim construction section. *See* PO Resp. 8–13 (citing *Cisco*, 767 F.3d 1308, 1317 n.1, and arguing for a direct requirement, without stating what “direct” means). These alleged disclaimers are not clear as discussed above. *See infra*, Section II.A.4.

Regarding Patent Owner’s related claim construction argument that Aventail Connect encrypts traffic, and the system routes traffic to Aventail’s ExtraNet proxy server, instead of the target, thereby showing a lack of a direct connection, the ’705 patent also initially directs all traffic to a proxy server, and the packets traverse randomly assigned routers along the path, with addresses that may change, as part of its “agile routing” feature—as opposed to specifying a target or involving a “normal” router function (which Patent Owner relies upon as a supposed distinction). *See* PO Resp. 36–37; Ex. 1050, 10:39–55, 40:7–8 (“DNS proxy 2610 intercepts all DNS lookup functions”), 40:24–25 (“The address that is returned need not be the actual address of the destination computer.”). The disclosed routers also decrypt packets along the way in a number of routers. *See* Ex. 1050, 10:8–15 (providing decryption of packets in routers, at least for addresses). As noted above, Patent Owner acknowledges that its claim construction

includes the traversal of routers, ISPs, gateways. The '705 patent also describes an intervening “load balancer that distributes packets across different transmission paths.” Ex. 1003, 6:11–12. And as noted, *Cisco* indicates that the claims do not preclude intermediate “VPN servers, VPN authentication servers, *proxy servers*, and firewalls.” *Cisco*, 767 F.3d at 1322 (emphasis added).

Petitioner also points to the “Extranet Neighborhood” feature as showing a direct connection. Pet. Reply 10 (citing Ex. 1009, 29, 60, 63 (figure), 90–101; Ex. 1005 ¶¶ 304–310, 420; Pet. 26). Petitioner contends that this feature shows direct access to hosts on a private network. *Id.* The record supports Petitioner. Aventail discloses that “you can connect your laptop through an Aventail ExtraNet Server to your internal company network” in order to browse files thereon. Ex. 1009, 90; Ex. 1005 ¶¶ 304–310, 420. It also discloses that “[u]sers can securely access computers from the desktop through Extranet Neighborhood.” Ex. 1009, 90. Dr. Tamassia explains that this connection would be the same as that with respect to users on a private network. Ex. 1005 ¶¶ 305, 310.

Therefore, even if a secure communication link as recited in claims 1 and 16, or a VPN link as recited in claims 6 and 21, requires a direct connection under a broadest reasonable construction of the terms, Petitioner shows sufficiently that the Aventail ExtraNet Server operates similarly to a router, firewall, or gateway to a private corporate network, and thereby provides a direct connection under reasoning in *Cisco*. See Pet. 20; Ex. 1009, 72–73; Ex. 1005 ¶¶ 200–07, 212, 220–26. Further, the record, which includes Patent Owner’s current arguments, some related prosecution history and district court litigation, and the '705 patent Specification, fail to

illuminate a clear interpretation of what a “direct” connection requires. See *supra* Section II.A.4 (Claim Construction).

iii. Remaining Limitations in Claims 1 and 16, and Challenged Dependent Claims 2, 3, 5, 6, 8–15, 17–19, 21, and 23–30

With respect to the remaining recited claim limitations, Petitioner sets forth detailed showings and rationale to support its challenge that the combination of Aventail, RFC 2401, and RFC 2543 would have rendered obvious independent claims 1 and 16 and dependent claims 2, 3, 5, 6, 8–15, 17–19, 21, 23, and 25–30. See Pet. 32–35, 41–52, and 55–58. For example, further addressing the “audio/video communications” element of claims 1 and 16, Petitioner relies on RFC 2543 to suggest multimedia applications in end-to-end encryption schemes like those suggested by the combination of Aventail and RFC 2401. See Pet. 47–48 (citing Ex. 1013, 1, 54, 137; Ex. 1005 ¶¶ 458–460; Ex. 1009, 27).

Petitioner also sets forth detailed showings and rationale to support its challenge that the combination of Aventail, RFC 2401, RFC 2543, and Brand would have rendered claim 24 obvious. See Pet. 58–59. For example, Petitioner relies on Brand to suggest an unmodulated transmission link as a known type of baseband link useful in networks such as Aventail’s network. See *id.* (citing Ex. 1012, 1:26–33, 17:44–46; Ex. 1005 ¶ 144).

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. Therefore, we determine that Petitioner has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found 1) dependent claims 1–3, 5, 6, 8–19, 21, 23,

and 25–30 obvious over the combination Aventail, RFC 2401, and RFC 2543, and 2) dependent claim 24 obvious over the combination Aventail, RFC 2401, RFC 2543, and Brand.

iv. Claims 4 and 20

Claims 4 and 20 require that the “determination” be made by a “server.” Petitioner contends that for purposes of claims 4 and 20, the SOCKS server makes the “determination.” Pet. 50. In addition to relying on its arguments with respect to claims 1 and 16, Patent Owner specifically relies on its argument discussed above that the SOCKS server does not make a determination. PO Resp. 38–39.

Relying on the combined teachings of Aventail, RFC 2401, and RFC 2543, Petitioner explains that Aventail’s SOCKS server (i.e., the Aventail ExtraNet Server) makes the claimed “determination” when it determines whether the client device is allowed access to the target device as part of the SOCKS negotiation. See Pet. 40–41; Ex. 1009, 5, 12; Ex. 1011, 19; Pet. Reply 11.

The record supports Petitioner’s analysis as set forth in our discussion above of claims 1 and 16. In summary, and by way of example, Aventail describes that the SOCKS server resolves the hostname in a proxy request, the SOCKS server engages in the negotiation process, and “[f]rom the application’s point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely TCP handshaking.” Ex. 1009, 12. The SOCKS server also selects the encryption module. *Id.* As also explained above, Aventail also describes how the server, in order to provide access for a specific client to a specific machine (i.e., make a determination), uses “rules for specifying which people and groups can access what machines and

services. Rule elements include: where they came from, the time of day, how they [are] authenticated, and encryption strength, etc.” Ex. 1011, 19. Further, “[t]he server checks client access requests against the access control rules . . . seeking a match between the request and the access requirements At the first instance of a match, the server stops searching and permits (or denies) access to the client.” *Id.*

In other words, Petitioner shows that, similar to the disclosed invention, Aventail’s SOCKS server employs matching rules with matching levels of security, including encryption strength, between requesting clients and a target, to determine access to the target, which constitutes the claimed determination by a server. As described above in connection with claims 1 and 16, RFC 2401 also suggests encryption for a target.

Therefore, 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 4 and 20 obvious over the combination of Aventail, RFC 2401, and RFC 2543.

v. Claims 7 and 22

Claims 7 and 22 recite that “the domain name is a secure domain name.” Dependent claim 7 depends from claim 3, which depends from claim 1. Claim 22 depends from claim 16. Claims 7 and 22 each recite that “wherein the domain name” recited in claims 1 and 16 is a “secure domain name.” As set forth above, a “secure domain name” is “a name that corresponds to a secure computer network address.” *Supra* Section II.A.3. Petitioner contends that “Aventail shows private domain name servers that are accessible only by way of a secure connection that is both authenticated and encrypted.” Pet. 53 (citing Ex. 1009, 73 (encryption and authentication

requirements), 74 (depicting a DNS server on the private network); Ex. 1005 ¶ 281). Petitioner also explains that “computers that have not created an authenticated and encrypted connection to the private network (via Aventail) will therefore not be able to resolve the domain names handled by the private domain name server of Aventail.” *Id.* (citing Ex. 1009, 72–74; Ex. 1005 ¶ 281).

Patent Owner argues that Petitioner’s “rationale is completely divorced from Petitioner’s analysis for independent claims 1 and 16.” PO Resp. 40. Patent Owner explains that Aventail does not disclose that the domain name submitted to the SOCKS server for resolution that Petitioner relies upon for claim 1 is resolved by the private DNS. *Id.* Patent Owner points out that “claims 7 and 22 reference *the* domain name recited in claims 1 and 16.” *Id.* Patent Owner also argues, based on its proposed construction, that the “secure domain name” must be “non-standard.” *Id.* at 37.

Patent Owner’s first argument is not persuasive, because Aventail describes that “the SOCKS server performs the hostname resolution” and shows a private DNS server for hostname resolution on the private network. Ex. 1009, 12, 72. As summarized above, Petitioner relies on the SOCKS server (a DNS) as one option with respect to claim 1. *See* Pet. 37–38. Sending that hostname to another internal server as another option (a private server behind a first SOCKS server) constitutes part of the same analysis. In addition, or alternatively, claims 1, 7, 16, and 22 do not require a private server or any server actually to resolve a secure domain name and return an IP address. Rather, the claims require the determination to be a result of the *request* to look up a secure domain—as opposed to a result of any particular

server actually resolving the request into an IP address. The '705 patent supports this interpretation. *See, e.g.*, Ex. 1050, 40:6–35 (returning a “host unknown” without necessarily looking up an IP address “if the user had requested lookup of a secure web site but lacked credentials”).

We also do not agree with Patent Owner’s second argument. As discussed above, our construction of “secure domain name” rejects Patent Owner’s argument that a secure domain name is a “non-standard domain name.” But even under Patent Owner’s proposed construction, Aventail discloses “non-standard” domain names. For example, Aventail explains that “[i]f the DNS proxy option is enabled and *the domain cannot be looked up directly*, Aventail Connect *creates a fake DNS entry* that it can recognize later, and returns this to the calling application.” Ex. 1009, 12 (emphasis added). The “fake DNS entry” constitutes a non-standard domain name, as it replaces a domain name, serves as a part of request to look it up that Aventail Connect proxies, and constitutes an artifice for a domain name that cannot be looked up. Also, the domain name that “cannot be looked up directly” constitutes a “non-standard” domain name, because it corresponds to a private device (represented by a fully qualified hostname) that the Aventail ExtraNet server must resolve. *See* Ex. 1009, 11–12. The Aventail ExtraNet server also acts as a firewall to a private network so that it would not be conventional under Patent Owner’s view. *See* Ex. 1009, 72–74.

The record supports Petitioner’s analysis including reasons for combining Aventail, RFC 2401, and 2543, which we adopt. Based on the foregoing discussion and the record, we determine that Petitioner has shown by a preponderance of the evidence that claims 7 and 22 would have been obvious over the combination of Aventail, RFC 2401, and RFC 2543.

III. MOTION TO EXCLUDE

Patent Owner filed a Motion to Exclude Exhibits 1001–04, 1006, 1007, 1017, 1019, 1022–41, 1044–49, 1051–54, 1057–60, 1063–65, 1067, 1069, and 1071, and portions of Exhibit 1005. Paper 30 (“Mot. to Exclude”), 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 *denied or dismissed* as moot.

A. Exhibits 1022, 1023, 1043, and 1057–1059

Patent Owner seeks to exclude Exhibits 1022, 1023, 1043, and 1057–59 (collectively, the “Aventail declaration testimony”) as inadmissible hearsay. Mot. to Exclude 2. As detailed above, Exhibit 1022 is the Chester Declaration, Exhibit 1023 is the Hopen Declaration, and Exhibit 1043 is the Fratto Declaration. The Petition relies on these to establish that Aventail is prior art. *See* Pet. 17–19. Also discussed above, Petitioner filed Exhibits 1057–1059 as supplemental information. *See* Paper 14, 17. Exhibit 1057 is the deposition transcript of Mr. Hopen from a district court proceeding, and Exhibit 1058 is a second declaration of Mr. Hopen from a reexamination proceeding. Exhibit 1059 is a portion of deposition testimony read into evidence in the above-mentioned district court trial. The exhibits are relevant to whether or not Aventail is prior art, as detailed above.

Although the Aventail declaration testimony originally was filed in other proceedings and not created specifically for this proceeding, the main distinction between it and the expert declaration testimony of Dr. Tamassia and Dr. Monroe is the caption. That difference is artificial because all of the declarations were filed in this proceeding, as if they were prepared for

this matter. Patent Owner chose not to seek the opportunity to cross examine the declaration testimony because, according to Patent Owner, “cross-examination . . . was not provided as routine discovery.” Paper 34 (“Reply to Opp. to Motion to Exclude”), 3; see 37 C.F.R. § 42.51(b)(ii). The latter contention is not persuasive, because Patent Owner could have sought to cross-examine these declarants, and had Petitioner not provided them, then could have sought to exclude their testimony.

Even if considered hearsay, Federal Rule of Evidence 807 provides a “residual exception” to the hearsay rule, which may apply even if no specific exception of Federal Rule of Evidence 803 applies. We determine that the exception applies here. To fall under this exception, the statement must satisfy the following requirements: 1) have equivalent circumstantial guarantees of trustworthiness; 2) be offered as evidence of a material fact; 3) be more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts; and 4) be in the interests of justice to admit. Fed. R. Evid. 807. The residual exception to the hearsay rule is to be reserved for “exceptional cases,” and is not “a broad license on trial judges to admit hearsay statements that do not fall within one of the other exceptions.” *Conoco Inc. v. Dep’t of Energy*, 99 F.3d 387, 392 (Fed. Cir. 1996), as amended on rehearing in part (Jan. 2, 1997) (internal quotations omitted). Trial courts are accorded wide discretion in applying the residual hearsay exception. *Doe v. United States*, 976 F.2d 1071, 1076–77 (7th Cir. 1992), *cert. denied* 510 U.S. 812 (1993); *United States v. North*, 910 F.2d 843, 909 (D.C. Cir. 1990), *cert. denied* 500 U.S. 941 (1991).

Petitioner responded to the objections by relying on Federal Rule of Evidence 807. Paper 33 (“Opp. to Mot. to Exclude”), 1–8. Petitioner analyzes each factor in detail. *Id.* We agree with and adopt Petitioner’s analysis. For example, we agree with Petitioner that the Aventail declaration testimony has the same circumstantial guarantees of trustworthiness as those declarations actually created for this proceeding. *See* Opp. to Mot. to Exclude 3–7. The vast majority of testimony in *inter partes* reviews is admitted in paper form, as a declaration, instead of as live witness testimony. Thus, whether or not testimony is specifically created for a specific IPR or is created for another proceeding, if the declaration is sworn testimony and the witness is available for cross-examination, the testimony bears the same guarantees of trustworthiness. *See also* Fed. R. Evid. 804(b)(1) (exception against the rule against hearsay for former testimony that “was given as a witness at a trial, hearing, or lawful deposition” and “is now offered against a party who an opportunity and similar motive to develop it by direct, cross-, or redirect examination”).

Patent Owner argues the exception should be used sparingly in exceptional cases. Mot. to Exclude 4. Patent Owner also criticizes the testimony of each witness. *Id.* at 2–4. For example, Patent Owner argues the declarations were prepared long after the event testified about, the January 1999 distribution of Aventail. *Id.* We found, above, that the testimony included documentation which corroborates the witnesses’ memory of the sequence of events. We are not persuaded by Patent Owner’s remaining arguments.

Petitioner's showing is persuasive. We adopt the showing by Petitioner, and for those reasons, we deny Patent Owner's Motion to Exclude Exhibits 1022, 1023, 1043, and 1057–1059.

B. Exhibits 1060 and 1063–65

Patent Owner seeks to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Mot. to Exclude 6–9. 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 this request as moot.

C. Exhibits 1001–1004, 1006, 1007, 1017, 1019, 1024–1035, 1037–1041, 1044–1049, 1051–1054, 1067, 1069, and 1071

Patent Owner seeks to exclude the above listed Exhibits as lacking relevance and as inadmissible hearsay. Mot. to Exclude 1–2, 9–10. Because we do not rely on the above listed Exhibits, we dismiss this request as moot.

D. Exhibit 1036

Patent Owner argues that “the Board should exclude Exhibits 1001–04, 1006, 1007, 1017, 1019, 1022–41, 1044–49, 1051–54, 1057–60, 1063–65, 1067, 1069, and 1071 because *one or more* of these [E]xhibits includes evidence that is inadmissible hearsay, evidence that is irrelevant to the instant proceeding, or evidence that lacks authentication. Mot. to Exclude 1 (emphasis added). Patent Owner also argues as follows: “Exhibits 1001–1004, 1006, 1007, 1017, 1019, 1024–1041, 1044–1049, 1051–1054, 1067, 1069, and 1071 should be excluded because they lack relevance.” *Id.* at 9.

As indicated in the first above-quoted argument, Patent Owner does not argue specifically that Exhibit 1036 includes evidence of hearsay, is irrelevant or lacks authentication, 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, or lacks relevance or

authenticity. *See* Paper 30, 1. Accordingly, Patent Owner fails to meet its burden on its Motion to Exclude Exhibit 1036 based on hearsay or authenticity. *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, but argues that "Petitioner does not even cite to these [E]xhibits." *Id.* at 10. 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.D, 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.

D. Portions of Exhibit 1005

Patent Owner seeks to exclude portions of Dr. Tamassia's testimony in Exhibit 1005 as lacking relevance because they relate to other proceedings. Mot. to Exclude 10. Patent Owner does not cite any specific paragraphs. *See id.* Because we do not rely on any paragraphs of Exhibit 1005 related only to other proceedings, we dismiss this request as moot.

IV. ORDER

For the reasons given, it is

ORDERED that claims 1–30 of the '705 patent are unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed as moot* in part and is *denied* in part; and

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

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@paulhastngs.com

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