

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00810
Patent 8,868,705

PATENT OWNER VIRNETX INC.'S NOTICE OF APPEAL

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
Madison Building East, 10B20
600 Dulany Street
Alexandria, VA 22314-5793


Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a), that Patent Owner VirnetX Inc. (“VirnetX”) appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered on August 30, 2016, (Paper 44) (the “Final Written Decision”) by the United States Patent and Trademark Office, Patent Trial and Appeal Board (the “Board”), and from all underlying orders, decisions, rulings, and opinions. A copy of the Final Written Decision is attached.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), VirnetX indicates that the issues on appeal include, but are not limited to, the Board’s determination of unpatentability of claims 1-34 of U.S. Patent No. 8,868,705 under 35 U.S.C. § 103, and any finding or determinations supporting or related to those rulings including, without limitation, the Board’s application of the broadest reasonable interpretation standard, the Board’s interpretations of the claim language, and the Board’s interpretation of the references.

Simultaneous with this submission, a copy of this Notice of Appeal is being filed with the Board. In addition, the Notice of Appeal and the required fee are

being filed electronically with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

Respectfully submitted this 31st day of October, 2016.

By: 

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for VirnetX Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that, in addition to being filed electronically through Patent Trial and Appeal Board End to End (PTAB E2E), the original version of this Notice of Appeal was filed by hand on October 31, 2016 with the Director of the United States Patent and Trademark Office, at the following address:

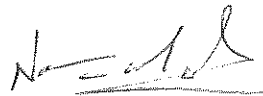
Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
Madison Building East, 10B20
600 Dulany Street
Alexandria, VA 22314-5793

The undersigned also certifies that a true and correct copy of this Notice of Appeal and the required fee were filed electronically via CM/ECF on October 31, 2016, with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

The undersigned also certifies that a true and correct copy of this Notice of Appeal was served on October 31, 2016 on counsel of record for Petitioner Apple Inc. by electronic mail (by agreement of the parties) at the following address:

iprnotices@sidley.com
Sidley Austin LLP
1501 K Street, N.W.
Washington, DC 20005

Date: October 31, 2016

By: 

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for VirnetX Inc.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00810
Patent 8,868,705 B2

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

ANDERSON, *Administrative Patent Judge*.

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–34 of U.S. Patent No. 8,868,705 B2 (Ex. 1001, “the ’705 patent”). VirnetX Inc. (“Patent Owner”)¹ filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). We have jurisdiction under 35 U.S.C. § 314. On September 11, 2015, we granted the Petition and instituted trial on claims 1–34 of the ’705 patent. Paper 8 (“Institution Decision” or “Dec. Inst.”)

After institution of trial, Patent Owner filed a Patent Owner Response (Paper 25, “PO Resp.”), and Petitioner filed a Reply (Paper 29, “Reply”). In addition, Petitioner proffered the Declaration of Dr. Roberto Tamassia (“Tamassia Declaration,” Ex. 1005). The deposition of Dr. Tamassia was taken by Patent Owner and filed by both parties. (“Tamassia Deposition,” Ex. 1068).² Patent Owner proffered the Declaration of Dr. Fabian Monroe. (“Monroe Declaration,” Ex. 2016).³ The deposition of Dr. Monroe was taken in this proceeding⁴ and in the ’237 IPR. (“Monroe Deposition,” Ex. 1066).

An oral hearing was held on June 8, 2016. The transcript of the hearing has been entered into the record. Paper 43 (“Tr.”).

¹ The Petition also names Science Application International Corporation as Patent Owner. However, the Patent Owner Response names only VirnetX.

² Patent Owner filed the Tamassia Deposition as Exhibit 2015. We refer only to Ex. 1068 unless otherwise noted.

³ Patent Owner also filed a Declaration of Dr. Monroe (Ex. 2001) from *Apple Inc. v. VirnetX Inc.*, IPR2014-00237 (“’237 IPR”). Patent Owner does not cite to Exhibit 2001.

⁴ The deposition of Dr. Monroe (Ex. 1067) from the ’237 IPR was also filed here by Patent Owner. Patent Owner does not cite to Exhibit 1067.

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We conclude, for the reasons that follow, that Petitioner has shown by a preponderance of the evidence that claims 1–34 of the '705 patent are unpatentable.

A. The '705 Patent

The '705 patent describes a system and method for transparently creating an encrypted communications channel between a client device and a target device. Ex. 1001, Abstract, Figs. 26, 27 (elements 2601, 2604). Secure communication is based on a protocol called the “Tunneled Agile Routing Protocol” or “TARP.” *Id.* at 3:16–19. Once the encrypted communications channel is created, the devices are configured to allow encrypted communications between themselves over the encrypted communications channel. *Id.* at 40:66–41:9. Figure 26 of the '705 patent is reproduced below.

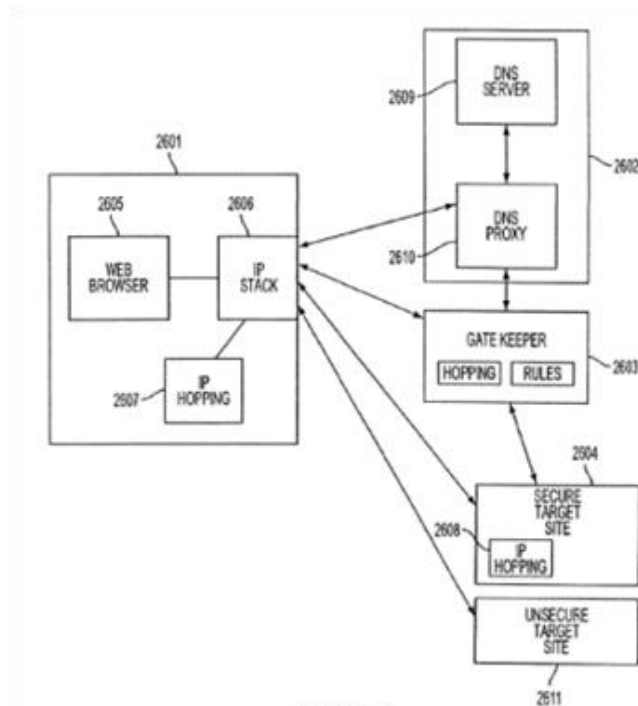


FIG. 26

Referring to Figure 26, user's computer 2601 is a conventional client, e.g., a web browser. Ex. 1001, 39:58–60. Gatekeeper server 2603 is interposed between modified Domain Name Server (“DNS”) 2602 and secure target site 2604. *Id.* at 39:62–66. The DNS includes both conventional DNS server function 2609 and DNS proxy 2610. *Id.* Conventional IP protocols allow access to unsecure target site 2611. *Id.* at 39:66–67.

In one described embodiment, establishing the encrypted communications channel includes intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device. Ex. 1001, 40:1–19. It further includes determining whether the request to look up the IP address corresponds to a device that accepts an encrypted channel connection with the client device. *Id.* at 40:1–29. Gatekeeper 2603 facilitates and allocates the exchange of information for secure communication, such as using “hopped” IP addresses. *Id.* at 40:32–35.

The DNS proxy server handles requests for DNS look-up for secure hosts. Ex. 1001, 40:43–45. If the host is secure, then it is determined whether the user is authorized to connect with the host. *Id.* at 40:51–53. If the user is authorized to connect, a secure Virtual Private Network (VPN) is established between the user's computer and the secure target site. *Id.* at 40:66–41:2.

B. Illustrative Claim

Petitioner challenges claims 1–34 of the '705 patent. Claim 1 is an independent method claim and claim 21 is an independent system claim. All

remaining claims depend directly or indirectly from claim 1 or 21. Claim 1 is reproduced below.

1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted⁵ in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

Ex. 1001, 55:43–67.

⁵ Patent Owner asserts “transmitted” was printed in error and that the claim was amended to include “intercepted” instead of “transmitted.” *See* Prelim. Resp. 29, n.3 (citing Ex. 1002, 638–639, 641, 655–656). In our Order dated December 9, 2015, (Paper 24) we authorized Patent Owner to file a request for a certificate of correction changing the word “transmitted” in claims 1 and 21 to “intercepted.” Paper 24, 3. In addition, as stipulated by the parties, we ordered that the change of wording does not affect the patentable significance of claims 1 and 21. *Id.*

C. Instituted Grounds of Unpatentability

We instituted on the following grounds asserted by Petitioner under 35 U.S.C. § 103: (1) claims 1–4, 6–10, 12–26, and 28–34 as unpatentable over Beser⁶ and RFC 2401;⁷ (2) claims 5, 11, and 27 as unpatentable over Beser, RFC 2401, and Brand.⁸ Dec. Inst. 23.

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. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142 (2016) (affirming the Patent Office’s authority to issue regulations establishing and governing *inter partes* review under 35 U.S.C. § 316(a)(4)). Under this standard, absent any special definitions, claim terms or phrases are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). The Board construed claim terms in a related patent in the Final Written Decision for the ’237 IPR. *See* ’237 IPR, (PTAB May 11, 2015) (Paper No. 41) (“’237 FWD”) (on appeal at the Federal Circuit). *See also VirnetX, Inc. v. Cisco Systems, Inc.*, 767

⁶ US 6,496,867 B1, issued Dec. 17, 2002, to Nurettin B. Beser and Michael Borella (“Beser,” Ex. 1007).

⁷ S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (“RFC 2401,” Ex. 1008).

⁸ US 5,237,566, issued Aug. 17, 1993, to Robert C. Brand and Stanford L. Mantiply (“Brand,” Ex. 1012).

F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents having similar claim terms).

Petitioner and Patent Owner each proffer proposed constructions of several claim terms. *See* Pet. 9–15; PO Resp. 1–17. Regardless of the preceding, Petitioner contends that the only terms Patent Owner argues are not disclosed by Besser and RFC 2401 are “secure domain name” and “intercepting.” Pet. Reply 1–2. Patent Owner disagrees with Petitioner and with the Institution Decision’s determination that no term requires construction. PO Resp. 1–2 (citing Dec. Inst. 8). Patent Owner identifies seven terms for construction. *Id.* at 3–17.

We have compared Patent Owner’s arguments in its Response to the terms it identifies for construction. Specifically, Patent Owner argues Besser and RFC 2401 do not disclose: (1) “intercepting from the client device a request to look up an Internet Protocol (IP) address;”⁹ and (2) “secure domain name.”¹⁰ No other argument in the Response is based on a term Patent Owner proposes for construction. We, therefore, agree with Petitioner that the only terms that may require construction are “intercepting from the client device a request to look up an Internet Protocol (IP) address” and “secure domain name.” *See* Pet. Reply 1–2. With respect to all other claim terms Patent Owner identifies for construction, our analysis is based on plain and ordinary meaning as understood by the person of ordinary skill in the art.

⁹ PO Resp. 21–27.

¹⁰ PO Resp. 33–34.

1. “intercepting from the client device a request to look up an Internet Protocol (IP) address” (claims 1 and 21)

Independent method claim 1 recites “*intercepting* from the client device *a request* to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device” (the “intercepting limitation”). Independent system claim 21 recites similarly “intercept from the client device a request to look up an Internet Protocol (IP) address.” Petitioner proposes a construction from the institution decision in the ’237 IPR, “receiving a request pertaining to a first entity at another entity.” Pet. 10–11. This construction was adopted in the Final Written Decision in the ’237 IPR. ’237 FWD 10–12.

Quoting Patent Owner in the ’237 IPR, we noted that Patent Owner “disagrees with this construction” (’237 PO Resp. 23), but “believes that no construction is necessary” (*id.* at 26), because “it does not appear that the construction of ‘intercepting’ will bear on the outcome of the issues in this *inter partes* review” (*id.* at 23). ’237 FWD 11. The ’237 IPR and this proceeding involve the same issue with respect to this term and the asserted prior art. Patent Owner does not dispute the relevance of the ’237 IPR, including the construction of the intercepting limitation. *See* PO Resp. 24, n5 (referencing our construction of the intercepting limitation in the ’237 IPR). Patent Owner states in the instant proceeding that “no construction is necessary.” PO Resp. 11. Nevertheless, Patent Owner urges that if we construe the term, then we should 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 channel.” *Id.*

To support its proposed alternative construction in this proceeding, Patent Owner argues 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. 12 (citing Prelim. Resp. 29–32;¹¹ Ex. 2016 ¶ 24). Patent Owner’s arguments and the record show that Patent Owner’s proposed construction adds unnecessary functionality to “intercepting a request” and violates the plain language of the claim. According to Patent Owner’s arguments, another recited phrase in claim 1 (and a similar phrase in claim 21), captures the functionality, in particular, the “determination” clause of claim 1. *Id.* More specifically, Patent Owner argues in the determination clause of claims 1 and 21 “a determination is made whether the request to look up the IP address corresponds to a device that accepts an encrypted channel connection with the client device, and that ‘in response to’ this determination, provisioning information required to initiate the encrypted communications channel is provided.” *Id.* We are not persuaded that functionality in another step of claim 1 supports Patent Owner’s proposal. Indeed, that the additional functionality Patent Owner proposes is covered elsewhere in the same claim would make Patent Owner’s proposed construction of the intercepting limitation duplicative and/or confusing.

The parties agree that the intercepting limitation (at least) involves receiving a request at some intermediate device. PO Resp. 11; Pet. 10–11.

¹¹ To the extent it attempts to do so, it is improper for Patent Owner to incorporate the Preliminary Response in its Response by reference. 37 C.F.R. § 42.6(a)(3). To the extent the arguments are repeated in the Response, they are proper and will be considered.

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). Pet. 10 (citing Ex. 1001, 39:1–3, 40:1–7, Figs. 26, 27). Furthermore, as quoted above, Patent Owner agreed in the ’237 IPR that Petitioner’s construction captured “the disclosed embodiments.” ’237 PO Resp. 26. In essence, Petitioner’s construction captures the notion of interception as disclosed in the ’705 patent, by requiring receiving to “pertain” to another entity.

Patent Owner alleges that Petitioner adopted an “intent” requirement in the “interception” clause. PO Resp. 23–24, n.5. Patent Owner points to a discussion by the Board in the ’237 IPR institution decision that Dr. Tamassia discusses. *Id.* at 24 (citing Ex. 2015, 80:3–13; Ex. 2016 ¶ 36); *see also id.* at 24, n.5 (citing ’237 IPR, Paper 15, 12). Petitioner disagrees with any intent requirement and contends that Patent Owner mischaracterizes Dr. Tamassia’s testimony. Pet. Reply 14–15.

Patent Owner only addresses this “intent” requirement in an attempt to distinguish its claims over the prior art and does not propose it as part of its claim construction. *See id.* at 23–24. Furthermore, any alleged prior requirement of “intent” did not survive to the ’237 FWD. *Compare* ’237 IPR, Paper 15 (institution decision), 13, *with* ’237 FWD 10–12. More importantly, Patent Owner does not allege or attempt to show that the ’705 patent supports or requires such “intent” as part of the broadest reasonable

construction of the intercepting limitation. The record fails to show support for it.¹²

Based on the foregoing discussion, the record shows that the additional functionality urged by Patent Owner should not be imported into the intercepting limitation, and Petitioner's construction tracks the claim and Specification. Accordingly, as set forth in the '237 FWD, the broadest reasonable construction of the intercepting limitation is "receiving a request pertaining to a first entity at another entity."

2. "*secure domain name*" (claims 3, 10, and 25)

Dependent claims 3 and 10 depend respectively from claims 1 and 8, which depends from claim 1. Claim 25 depends from claim 21. Claims 3, 10, and 25 each recite "wherein the domain name is a secure domain name." Relying, in part, on a related *inter partes* proceeding, Petitioner argues "secure domain name" is "a name that corresponds to a secure computer network address." Pet. 11–12 (citing IPR2015-00481).¹³ Petitioner contends its proposed construction is consistent with the Specification. *Id.* at 12 (citing Ex. 1001, 51:6–42 ("a 'secure domain name' [is] a domain name that corresponds to the secure network address of a secure server 3320")).

¹² Although not part of the claim construction, a requestor may "intend" for the entered domain name in a request to reach the target device, but the DNS intercepts it to perform the look up. *See, e.g.*, Ex. 1001, 39:41–46 ("DNS server traps DNS requests"), *id.* at 39:64–66 ("A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2701.").

¹³ The full citation is *Apple Inc. v. Virnetx, Inc.*, IPR2014-00481 ("481 IPR"), slip. op. at 8 (PTAB Sept. 3, 2014) (Paper 11); *see also* '481 IPR, Final Written Decision, at 13–14 (Paper 35) (declining to modify construction).

Petitioner notes additional disclosure from the Specification in support of its construction. *Id.* (citing Ex. 1001, 40:1–7, 7:39–42). Finally, Petitioner refers to testimony from the Tamassia Declaration, which relies on the same portions of the Specification to conclude that the term has “a more general meaning of being a name that corresponds to a particular device on a secure computer network (i.e., one that would have an address on that secure computer network).” *Id.* (citing Ex. 1005 ¶ 73).

Patent Owner acknowledges Petitioner’s proposed construction was adopted in the ’237 IPR. PO Resp. 4.¹⁴ However, Patent Owner argues “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.* at 3 (Table). Patent Owner argues its proposed construction was an agreed construction from the related district court litigation. *Id.* at 4 (citing *Virnetx Inc. v. Apple Inc.*, Case 6:10-cv-00417-LED (E.D. Tex., Dec. 21, 2011), Joint Claim Construction Chart, 19–20, Ex. 2002). PO Resp. 4. Patent Owner cites to the Specification as also supporting its proposal, specifically including that the “secure domain name” is a “nonstandard domain name.” *Id.* (citing Ex. 1001, 7:29–31, 7:39–42, 50:22–31, 51:6–10, Figs. 33–34). Testimony from the Monroe Declaration ’810 is also cited as support that “SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses.” *Id.* (citing Ex. 2016 ¶¶ 15–16).¹⁵

¹⁴ The ’237 IPR construction of “secure domain name” is the same as the construction in the ’481 IPR cited above by Petitioner.

¹⁵ The cited portion of the Monroe Declaration includes quotes from the ’705 Patent. The Monroe Declaration does conclude, based on the Specification, that “[o]ne of ordinary skill in the art would understand based

Patent Owner further contends it disclaimed Petitioner’s proposed construction in a now completed *inter partes* reexamination of a related patent. PO Resp. 5 (citing Control No. 95/001,270, Response to Office Action, 5 (Apr. 19, 2010), Ex. 2008; Control No. 95/001,270, Right of Appeal Notice, 4 (Dec. 3, 2010), Ex. 2006). Patent Owner acknowledges this is a prosecution history estoppel argument which “generally binds only the patent owner.” *Id.* at 6–7 (citing *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 978 (Fed. Cir. 2014)). Patent Owner urges the prosecution history should be consulted in subsequent reviews of the patent in determining the broadest reasonable interpretation. *Id.* at 7 (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)).

We start with the language of claims 3, 10, and 25. These dependent claims recite that the domain name is a “secure domain name.” The plain meaning of those words is found in Petitioner’s proposed construction, “a name that corresponds to a *secure* computer network address.” The language is clear and straightforward and any construction under the broadest reasonable interpretation standard should not lead us away from that clarity. *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

on the disclosure of the ’705 patent that to obtain the URL for a ‘secure domain name,’ ‘a secure domain name service (SDNS)’ must be queried.” Ex. 2016 ¶ 17. This opinion is not supportive of the proposed construction.

application of the widely accepted meaning of commonly understood words.”).

We turn now to the Specification. The patent 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 states that “[a]lternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name.” Ex. 1001, 50:29–31. The column 50 quote follows a description of standard domain names like .com, including adding “s” for secure. *Id.* In addition to the preceding, the Specification discloses an example of “replac[ing] the top-level domain name . . . with a secure top-level domain name.” Ex. 1001, 50:22–25, *see also id.* at 51:6–42 (a “secure domain name” is a domain name that corresponds to the secure network address of a secure server 3320), *id.* at 40:1–7 (evaluating domain names in DNS requests to determine whether access to a secure site has been requested), *id.* at 7:39–42 (“Each secure computer network address is based on a non-standard top-level domain name, such as .scom,.sorg, .snet, .sedu, .smil and .sint.”). Thus, the Specification does not expressly state that the “secure domain name” *must* be “non-standard,” only that it is secure, which is encompassed in Petitioner’s proposed construction.

Next we address Patent Owner’s prosecution history estoppel argument. There is nothing in the Federal Circuit case law which dictates

that prosecution history is anything more than something to be consulted in claim interpretation. *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, 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.”).

The Specification and claims record do not support the prosecution history arguments. The plain language of the claims outweighs the arguments made. For example, Patent Owner contends that Patentee 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. *See* PO Resp. 5 (citing Response to Office Action in control No. 95/001,270 (Apr. 19, 2010), 5 (Ex. 2008)). It is not clear how this argument creates a distinction, or what “just happens to be associated with a secure computer” means, but Patent Owner appears to contend it means “a secure domain name cannot be resolved by a conventional domain name service.”¹⁶ *See* PO Resp. 5; Ex. 2008, 6 (arguing

¹⁶ 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

“a secure domain name cannot be resolved by a conventional domain name service, for example, but relying on “the inventors . . . acting as their own lexicographers” and citing disclosed examples in the ’180 patent of non-standard top-level domain names).

Nothing in the ’705 (or ’180) patent requires a conventional DNS not to return an address for all of the disclosed secure domain names, for example, if the name happens to be listed in that DNS and also another DNS, such as a secure DNS. A conventional DNS function involves resolving names into addresses. *See* Ex. 1005 ¶¶ 126–27 (“much like a file system”), 304–08 (citing Ex. 1001, 39:1–3 (describing Conventional DNS functionality)). The ’705 patent contemplates returning different addresses for the same domain name based on a user’s security levels, identity, and/or subscription level, , and combining conventional DNS and proxy functions. Ex. 1001, 40:20–29, 38–40, 51–57, 51:6–27. Furthermore, rather than not returning a secure domain name from a conventional DNS based on the type of name itself, the Specification states that a “DNS *proxy*” returns a “host-unknown” “if the user had requested lookup of a secure web site *but lacked credentials to create such a connection.*” *Id.* at 40:24–27 (emphases added).

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. 2006, 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.* The cited examples do not support a clear disclaimer that distinguishes a “secure domain name” from a secure domain name that happens to correspond to a secure computer. *See id.* These passages describe examples that correspond to a non-standard top-level domain name. *See* ’180 patent, 51:25–53.

Patentee's 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 indicates (Ex. 2008, 6) that the disclaimer argument does not pass muster. Patent Owner does not argue here that the '705 patent supports a lexicographic definition for all its disclosed secure domain names based on unclaimed examples related to top-level secure domain names.

Furthermore, Petitioner contends that Patent Owner argued during prosecution of a related patent that the term "secure name" encompassed a "secure non-standard domain name" such as "a secure nonstandard top-level domain name (*e.g.*, .scom) or a **telephone number**." Pet. Reply 16 (citing Ex. 1069, 9). The cited prosecution history 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 secure name:

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

Ex. 1069, 9 (emphasis added).

Patent Owner does not demonstrate that the Specification requires a secure domain name to be "top-level" or "non-standard." And more importantly, setting aside the top-level domain names, which are mere

examples that Patent Owner does not rely on as part of its proposed claim construction, Patent Owner fails to explain clearly what the term “non-standard” means or how a “non-standard” domain name differs from a “secure computer network address.” As discussed below, even if we adopted Patent Owner’s narrower claim construction, as supported by the prosecution history, our obviousness analysis would remain unchanged. We determine that the prosecution history argument is not supported by the Specification and is outweighed by the plain language of the claim.

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.’” IPR2014-00481, Paper 35, 13 (quoting ’481 IPR Ex. 1018, 18 (district court findings and rationale)).¹⁷ The record here supports the argument made by Patent Owner in the district court—the Specification and prosecution history do not support the non-standard distinction.

Neither are we persuaded that what the parties agreed to in the district court binds us. First, Petitioner does not agree to that construction in this proceeding. We are unaware of any precedent preventing Petitioner from taking inconsistent positions in different forums and Patent Owner does not cite any either. Further, as has now been confirmed in *Cuozzo*, we apply the broadest reasonable interpretation standard and not the litigation standard in

¹⁷ The district court case cited in the ’481 IPR involved a finding of a disclaimer of a different but related term: “secure domain name service.” See ’481 IPR, Ex. 1018, 17–18; ’481 IPR, Ex. 2003, 91.

district court. On the other hand, the construction Petitioner now proposes is taken directly from other *inter partes* reviews. These circumstances are adequate justification for a differing construction from that of the district court.

In addition to the preceding reasons, we agree with the analysis made in the construction of “secure domain name” in a prior *inter partes* review proceeding. *See* ’481 IPR, Paper 35, 13–14. Thus, we construe “secure domain name” as “a name that corresponds to a secure computer network address.”

OBVIOUSNESS-BESER AND RFC 2401

Petitioner alleges claims 1–4, 6–10, 12–26, and 28–34 would have been obvious over Beser and RFC 2401. Pet. 24–51. Petitioner’s evidence includes the Tamassia Declaration. Ex. 1005 ¶¶ 274–364, 383–403). Patent Owner argues the challenged claims are patentable. PO Resp. 17–39. Patent Owner’s evidence includes the Monroe Declaration ’810.¹⁸ Ex. 2001 ¶¶ 31–63.

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 ¶ 110; *see* Pet. 8–9. 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. *Id.*

¹⁸Patent Owner also provides the Monroe Declaration ’237 but does not cite to it in the Response.

Patent Owner argues that “Petitioner proposes a lower level of skill, but Patent Owner’s proposed level is the same level of skill that Petitioner and nearly a dozen other parties have consistently advocated in related litigation involving patents in the same family” as the ’705 patent. Prelim. Resp. 23¹⁹ (citing Ex. 2005, 4; Ex. 2004, 5). Patent Owner’s expert, 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. 2016 ¶ 13. Dr. Monroe adds that his “view is consistent with VirnetX’s view that a person of ordinary skill in the art requires a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security.” *Id.*

We are persuaded that Patent Owner’s description of the background of a person of ordinary skill in the art is not lower than or 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.

¹⁹ Patent Owner does not appear to renew this argument in its Response. *See* PO Resp. 9–10 n.3.

*C. Tamassia Declaration*²⁰

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. 47. 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.'" Reply 23 (citing Fed. R. Evid. 702). Petitioner adds that "no rule requires an expert to opine on the ultimate question of obviousness or on every potentially relevant fact at issue for his opinion to be admissible or entitled to weight." *Id.* at 23–24.

Patent Owner has not articulated a persuasive reason for giving Dr. Tamassia's declaration, as a whole, little or no weight in our analysis. We agree with Petitioner that experts are not required to opine on every relevant factual and legal issue in order to be accorded substantial weight. The cases Patent Owner relies on do not persuade us otherwise. For example, Patent Owner cites *Schumer v. Laboratory Computer Systems, Inc.*, 308 F.3d 1304, 1315 (Fed. Cir. 2002), for the proposition that "expert testimony 'must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference.'" PO Resp. 48. 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:

²⁰ We address Patent Owner's motion to exclude certain paragraphs of Exhibit 1005 in a separate section, below.

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

Schumer, 308 F.3d at 1315–16 (emphasis added). 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.* 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 RFC 2401

Patent Owner asserts that Petitioner has not sufficiently established that RFC 2401 qualifies as a printed publication as of its alleged publication date. PO Resp. 39–47. We look to the underlying facts to make a legal determination as to whether a document is a printed publication. *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1364 (Fed. Cir. 2014). 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.*, 752 F.3d at 1364. To qualify as a printed publication, a document “must have been sufficiently accessible to the public interested in the art.” *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009).

In our Decision to Institute, we found that RFC 2401 included indicia suggesting a reasonable likelihood that the document was made public because (1) RFC 2401 is a dated “Request for Comments” from the “Network Working Group,” discussing a particular standardized security protocol for the Internet, and (2) it describes itself as a “document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. . . . Distribution of this memo is unlimited.” Dec. Inst., 9 (citing Ex 1008, 1). On this basis,

we determined that Petitioner had met its burden for a threshold showing to proceed to trial. *Id.*

In support of Petitioner’s position, the testimony from the Tamassia Declaration is 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 ¶ 148. Dr. Tamassia goes on to discuss an RFC that discusses the RFC development and publication process itself—RFC 2026, dated October 1996. *Id.* ¶¶ 149–155; Ex. 1036. Dr. Tamassia testifies 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.* ¶ 152. RFC 2026 also explains that anyone can obtain RFCs from a number of Internet hosts and each RFC “is made available for review via world-wide on-line directories.” *Id.* ¶¶ 148–49; Ex. 1036, 5–6.

Patent Owner argues that Petitioner cannot rely on evidence it has proffered to support this finding. First, Patent Owner argues that testimony by Dr. Tamassia should not be accorded any weight because Dr. Tamassia has not been established to have personal knowledge that RFC 2401 was actually released to the public in November 1998, nor has Dr. Tamassia “been established as someone familiar with, let alone an expert in, the workings of the Internet Engineering Task Force (IETF)—the body responsible for the RFCs.” PO Resp. 40–41.²¹

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. 40 n.6. Patent Owner, itself, however, directed the Board’s attention to this testimony in its Preliminary Response (Paper 6, 3–4), and thus clearly

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), which is not objected to by Patent Owner and is evidence of record. As part of routine discovery (37 C.F.R. § 42.51(b)(1)(ii)), Patent Owner had the opportunity to cross-examine Dr. Tamassia and did so, taking the Tamassia Deposition and making it of record. *See* Ex. 2015. Patent Owner does not point us to any discussion of this issue in the Tamassia Deposition. RFC 2401's contents are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including a date "November 1998" indicated on the top right corner of the first page of the document. Moreover, a request for suggestions and improvements for an Internet standards protocol, having no indication of being a mere draft or internal paper, is the type of document whose very purpose is public disclosure.

"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)). We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401(dated November 1998) was sufficiently disseminated to persons of ordinary skill interested in computer networking and security to be deemed "publicly accessible" at the relevant time.

has had adequate notice of its contents such that it may respond with no issues of prejudice.

Therefore, on this record, we determine RFC 2401 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

E. Overview of Beser

Beser describes a system that establishes an IP (internet protocol) tunneling association on a public network between two end devices. *See Ex. 1007, Abs.* Figure 1 of Beser is reproduced below.

FIG. 1

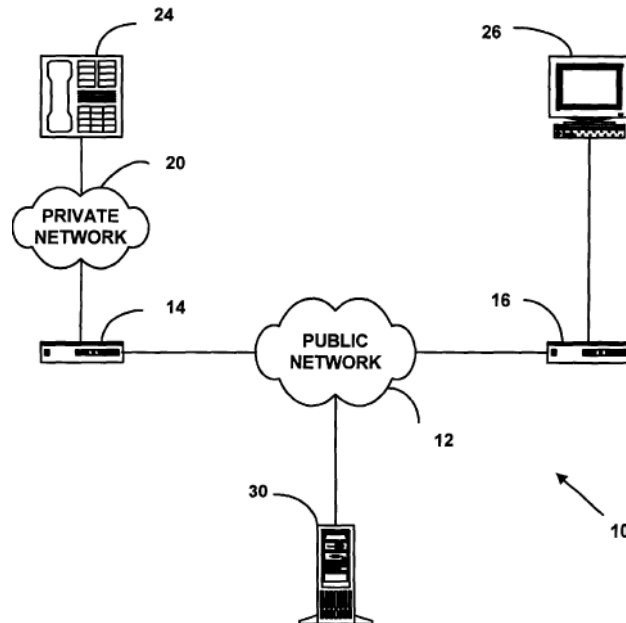


Figure 1 of Beser illustrates a network system, including public network 12, network devices 24 and 26, private network 20, trusted third-party network device 30, and modified routers or gateways 14 and 16. *Ex. 1007, 3:60–4:18.* Beser describes network devices 24 and 26 as telephony devices, multimedia devices, VoIP devices, or personal computers. *Id.* at 4:43–52.

Beser’s system “increases the security of communication on the data network” by providing and hiding, in packets, “private addresses” for originating device 24 and terminating device 26 on the network. *See id.* at

Abs., Figs. 1, 6. To begin a secure transaction, requesting device 24 sends a request to initiate a tunneling connection to network device 14. *Id.* at 8:21–47. This request includes a unique identifier for the terminating end of the tunneling association—terminating device 26. *Id.* at 7:64–8:3. The packets used to transfer this unique identifier across the public network “may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12.” *Id.* at 11:22–25. Beser discloses, as background prior art, known forms of encryption for the information inside these packets, including IP Security (“IPSec”). *Id.* at 1:54–56. Once network device 14 receives the request, it passes the request on to trusted-third-party network device 30. *Id.* at 8:3–4, 8:48–9:5.

Trusted-third-party network device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network device 16 and terminating devices 26. *See id.* at 11:32–58. DNS 30 associates terminating network device 26, based on its unique identifier in the request, with a public IP address for router device 16. *See id.* at 11:26–36. Trusted-third-party network device 30 then assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *Id.* at 9:29–35, 12:16–19. The negotiated private IP addresses are “isolated from a public network such as the Internet,” and “are not globally routable.” *Id.* at 11:62–65.

F. Overview of RFC 2401

RFC 2401 describes the 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.*

G. Claims 1 and 21

Although claim 1 recites “a method of transparently creating an encrypted communications channel” and claim 21 recites “a system for transparently creating an encrypted communications channel,” the two claims encompass substantially the same subject matter. Both Petitioner and Patent Owner argue claims 1 and 21 together. Pet. 30–41; PO Resp. 21–33 (Patent Owner includes claims 2–4, 6–10, 12–20, 22–26, and 28–34 in its argument, the only limitations argued are from claims 1 and 21); Reply 2–15. We, therefore, analyze the two independent claims 1 and 21 together.

1. Petitioner’s Assertions

Petitioner asserts that the “non-encrypted streaming audio/video example” described in *Beser* teaches each of the limitations of claims 1 and 21 except the required “encrypted communications channel.” Pet. 30–32, 34–41. Specifically, as per the preamble of claim 1,²² Petitioner argues that

²² Petitioner proceeds on the basis that the preamble is limiting. Patent Owner does not make a contrary argument. The preamble recites, in part, . . . “an encrypted communications channel between a client device and a target device,” which provides antecedent basis for those terms. We agree the preamble is limiting.

Beser's originating end device (Ex. 1007, Fig. 1 element 24) is equivalent to the claimed client device and Beser's terminating end device (Ex. 1007, Fig. 1, element 26) is equivalent to the claimed target device. *Id.* at 16, 31 (citing Ex. 1007, 8:15–20, 21:52–62, 22:2–22, Ex. 1005 ¶¶ 274, 342–43).

Petitioner also argues that Beser discloses step (1) of claim 1, “intercept[ing] . . . a request to look up an [] IP address corresponding to a domain name associated with the target” Pet. 32–34. Petitioner cites to Beser's teaching that the originating end device (“*client device*”) sends a request to initiate a tunneling association with the terminating end device (“*target device*”). *Id.* at 32 (citing Ex. 1007, 7:64–8:1, 9:64–10:41; Ex. 1005 ¶ 316). The request will be received “not by the terminating end device, but by a first network device, which evaluates all of the data packets it receives (i.e., the request is “intercepted” by the first network device).” *Id.* at 32–33 (citing Ex. 1007, 8:21–47; Ex. 1005 ¶¶ 299–300, 317, 322). Once the trusted-third-party network device receives, i.e., “intercepts,” the request containing unique identifier in the form of a domain name, it looks up the IP address associated with the domain name. *Id.* at 33 (citing Ex. 1007, 4:8–11, 8:4–7, 10:38–41, 11:26–55; Ex. 1005 ¶¶ 310, 323–325). Petitioner also asserts that “Beser . . . shows that, even though the request contains a unique identifier associated with the terminating end device, the request is actually ‘intercepted’ by each of the first network device and the trusted-third-party network device because they each receive ‘a request pertaining to a first entity at another entity.’” *Id.* (citing Ex. 1007, 8:21–47; Ex. 1005 ¶ 69).

Step (2) of claim 1 recites “determining whether the request to look up the IP address in step (1) corresponds to a device that accepts an encrypted

channel connection with the client device.” As noted above, Petitioner asserts the following:

[T]he Beser streaming video or audio example does not necessarily encrypt all the IP traffic sent over the secure tunnel. This distinction would have been considered an obvious variation of the Beser scheme when considered with RFC 2401.

Pet. 34. Specifically, Petitioner asserts Beser teaches determining whether access to a secure site has been requested. *Id.* (citing Ex. 1001, 40:1–7; *Apple Inc. v. VirnetX Inc.*, IPR2014-00237, slip op. at 7 (PTAB May 14, 2014) (Paper 15)). Petitioner explains that Beser teaches establishing a secure tunnel between the first (client) and second (target) devices. *Id.* at 35 (citing Ex. 1007, 9:6–11, 9:26–30, 11:9–44; Ex. 1005 ¶¶ 324, 330).

Petitioner concludes that “a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401.” *Id.* at 36–37 (citing Ex. 1007, 1:54–56, 11:26–58; *see also* Ex. 1005 ¶¶ 323–325, 330, 393, 395, 398–399).

Step (3) of claim 1 recites, in pertinent part, in response to step (2), “providing ‘*provisioning information required to initiate . . . [an] encrypted communications channel.*” Noting that Beser does not necessarily use encryption in the streaming of audio or video data, Petitioner relies on RFC 2401 to show the encryption feature of the limitation. Pet. 37. Petitioner concludes that Beser in view of RFC 2401 would therefore have rendered obvious the creation of an “encrypted communications channel.” *Id.*

According to Petitioner, it would have been obvious to a person of ordinary skill in the art to encrypt the traffic being sent in Beser using the teachings of RFC 2401. Pet. 26–27 (citing Ex. 1007, 1:54–56; Ex. 1005

¶¶ 383–385, 395). Petitioner argues that “a person of ordinary skill would have considered the teachings of Beser in conjunction with those in RFC 2401 because Beser expressly refers to the IPsec protocol (which is defined in RFC 2401) as being the conventional way that the IP tunnels described in Beser are established. *Id.* at 27 (citing Ex. 1007, 1:54–56; Ex. 1005 ¶¶ 383–385, 395). Petitioner adds that Beser also indicates that “its IP tunneling schemes are compliant with standards-based processes and techniques (e.g., IPsec), and can be implemented using pre-existing equipment and systems” and that “IP tunnels are and should ordinarily be encrypted.” *Id.* (citing Ex. 1007, 1:54–56, 4:55–5:2, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 282–283, 285, 383–386, 389–390, 394, 398).

Petitioner asserts the person of ordinary skill would have been motivated “to encrypt IP traffic within the IP tunnel of Beser pursuant to the guidance in RFC 2401, which describes the IPsec protocol referenced in Beser.” *Id.* at 28 (citing Ex. 1005 ¶¶ 389–390, 393, 399; Ex. 1007, 1:54–56; Ex. 1008). Petitioner points to “case 3” of RFC 2401 disclosing “the same network topology as Beser, with one tunnel between two security gateways such as edge routers, and another tunnel between the two end devices.” *Id.* (comparing Ex. 1008, 25 with Ex. 1007, Fig. 1, Ex. 1005 ¶¶ 396–397). The combination of Beser and RFC 2401 would achieve end-to-end encryption hiding both the source and destination addresses. *Id.* (citing Ex. 1005 ¶ 399).

According to Petitioner, Beser promotes the use of encryption over prior art that prevents encryption. Pet. 29 (citing Ex. 1007, 2:22–27, 11:22–25, 18:2–5, 20:11–14). Petitioner also contends the IPsec protocol was known to be “highly adaptable, enabling it to accommodate computational

burdens of a particular configuration by adjusting parameters of the IPsec protocol (e.g., adjusting the strength or type of encryption used).” *Id.* at 29–30 (citing Ex. 1008, 4, 7, 10). Petitioner concludes:

Accordingly, a person of ordinary skill would have considered Beser in conjunction with RFC 2401 in February 2000. Ex. 1005 at ¶¶ 393, 399. When so considered, the person of ordinary skill would have found it obvious to encrypt the IP traffic being sent over the Beser secure IP tunnel, even in the streaming video or audio applications discussed in Beser. Ex. 1005 at ¶¶ 389, 393, 399.

Id. at 30.

2. Patent Owner’s Assertions

In general, Patent Owner contends that Beser alone does not disclose encryption but uses a “tunneling association.” PO Resp. 18 (citing Ex. 1007, 3:1–9, Ex. 2016 ¶ 26). As discussed above, the Petition acknowledges the Beser IP tunneling scheme does not include encryption expressly of data but cites to RFC 2401 as teaching encryption. Pet. 36–37.

Patent Owner does not dispute every allegation made in the Petition relating to the steps of claim 1 or the limitations of claim 21. As detailed above, we have reviewed the evidence and argument of the undisputed allegations. We find that Petitioner has shown by a preponderance of the evidence that those steps and limitations which are not disputed in the Response are disclosed by Beser in combination with RFC 2401.

The only limitation of claims 1 and 21 Patent Owner contests is “intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device.” See PO Resp. 21. This is the limitation in step (1) of claim 1 and limitation (1) of claim 21. In section II.A.1. above we construed

“intercepting from the client device a request to look up an Internet Protocol (IP) address” to mean “receiving a request pertaining to a first entity at another entity.”

Patent Owner contends the above limitation is not disclosed by Beser in combination with RFC 2401. PO Resp. 21–27. Specifically, Patent Owner makes two arguments, i.e., that “Beser’s request, however, is not a ‘request to look up an Internet Protocol (IP) address’ and is not ‘intercept[ed].’” *Id.* at 21 (citing Ex. 2016 ¶ 31). Each argument is addressed below.

a. Request to Look Up an Internet Protocol (IP) Address

Patent Owner’s first argument is that Beser does not teach a “request to look up an Internet Protocol (IP) address.” PO Resp. 22–23. Some of Patent Owner’s arguments are based on Beser’s Figure 6, reproduced in the Response at page 20 and below:

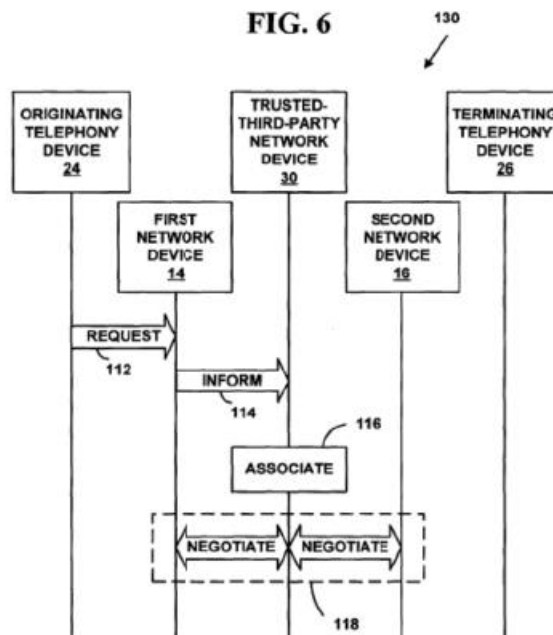


Figure 6 of Beser illustrates first and second network devices 14 and 16, originating device 24, terminating telephony device 26, and trusted third-party network device 30. *See* Ex. 1007, 11:59–12:27.

As a result of a negotiation between the trusted-third-party device and first and second network devices 14 and 16, each device 24 and 26 is assigned private IP address 50. *Id.* at 11:59–12:4.²³ Thus, trusted third-party network device 30 may “ensure anonymity of the telephony devices (24, 26).” *Id.* at 12:16–19.

Patent Owner argues that Beser requests to “initiate a tunneling connection” and does not “request to look up an Internet Protocol (IP) address.” PO Resp. 22 (citing Ex. 2016 ¶ 32). Patent Owner asserts the Petition is incorrect in alleging that “the trusted-third-party network device in Beser will ‘look up and return to the first network device’ a ‘public IP address for the second network device.’” PO Resp. 22–23 (citing Pet. 34). Patent Owner argues private IP addresses are negotiated between the first (originating) device and the second (terminating) device and not the trusted-third-party device. *Id.* at 22 (citing Ex. 1007, 8:9–15, 11:58, Fig. 6 (step 118), Ex. 2016 ¶ 33). Additionally, Patent Owner contends the negotiation is not a “look up” but rather an “assignment” of IP addresses. *Id.* (citing Ex. 1007, 12:2–4, Ex. 2016 ¶ 33).

Patent Owner also disputes the assertion in the Petition that Beser’s disclosure of a database entry in the trusted-third-party network device will “look up and return to the first network device” a “public IP address for the second network device.” PO Resp. 22–23 (citing Pet. 34). Patent Owner

²³ Note “negotiate” arrows in Figure 6 above. *See also* Pet. Reply 8–9 (citing *inter alia* Ex. 1007, Fig. 6, Pet. 21).

argues that the trusted-third-party device “may include a public IP 58 address for the terminating telephony device 26.” *Id.* at 23 (citing Ex. 1007, 11:50–55). Patent Owner contends there is no suggestion that there is a lookup when the tunnel request is received at the trusted-third-party device or at the terminating device. *Id.* Rather, “Beser only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, it associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26.” *Id.* (citing Ex. 1007, 11:26–32; Ex. 2016 ¶ 34). Patent Owner also suggests the Beser tunneling request cannot be one to “lookup an IP address” because trusted device 30 looks up the public IP address of second network device 16 instead of terminating device 26. *Id.* at 23.

Petitioner argues the first interception occurs when a data packet is received by the first network device, which determines the data packet can be forwarded to a conventional DNS server, which is associated with a public IP address. Pet. 32–33 (citing Ex. 1007, 4:7–42, 8:39–44; Ex. 1005 ¶ 300). Petitioner explains that Beser teaches that, if special handling of the data packet is required (“*e.g.*, due to the presence in it of a distinctive sequence of bits in the datagram”), the first network device forwards the data packet to trusted-third-party device 30, which “looks up” an IP address. *Id.* at 33 (citing Ex. 1007 at 8:21–47; Ex. 1005 ¶ 322). Petitioner further explains that in this second “interception,” the tunneling request includes a unique identifier, a private IP address for terminating device 26. *Id.* at 33–34 (citing Ex. 1007, 8:1–3, 10:37–42; Ex. 1005 ¶¶ 318–19); *see also* Pet. Reply 8–9 (citing Ex. 1007, 11:45–58, 9:29–30, 12:16–19, 14:14–27, Figs. 6, 9). As a result, “the private IP addresses for the originating and

terminating end devices will be used to establish a virtual tunneling association and transmit data between the end devices over a public network, providing anonymity.” *Id.* at 21–22 (citing Ex. 1007, 8:12–20, 11:59–62, 12:28–32; Ex. 1005 ¶¶ 342–44); *see also* Pet. Reply 9 (citing Ex. 1007, 21:48–52). Petitioner alleges Beser teaches that trusted device 30 receives the tunneling request, and in response, it associates an IP address with the unique identifier by looking it up in its internal database. Pet. Reply 10 (citing Ex. 1007, 11:9–20, 11:26–58).

In addition to those two IP addresses, Petitioner also contends that Patent Owner “admits that trusted device 30 contains a database or similar structure that correlates each unique identifier to the public IP addresses of second network device 16 and terminating device 26.” Pet. Reply 9 (citing PO Resp. 23). In its Response, Patent Owner states that “*Beser* simply states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26.” PO Resp. 23 (citing Ex. 1007, 11:50–55). However, Patent Owner contends that “*Beser* never suggests that this data structure is looked up.” *Id.*

We agree with Petitioner’s analysis and determine that Petitioner has shown, by a preponderance of the evidence, that Beser’s tunneling request discloses the claimed request to look up an IP address. Contrary to Patent Owner’s argument as quoted in the previous paragraph, we find that Beser implies looking up the public IP 58 address for terminating telephony device 26 to create its tunneling association. *See* Ex. 1007, 11:50–55; Ex. 1001 ¶ 308 (describing mapping associations for a number of IP addresses, including “the IP address of the end device”). As Dr. Tamassia testifies, it was well-known that DNSs respond to look up requests by

providing IP address data. Ex. 1005 ¶¶ 126, 304–308 (citing Ex. 1001, 39:1–3 (describing Conventional DNS functionality)).

In addition to looking up the public IP address of terminating device 26, as the Tamassia Declaration also explains, Beser’s “trusted-third-party network device receives a request to initiate a tunneling association, it uses the unique identifier in the request to look up an Internet Protocol (IP) address in the database of unique identifiers.” Ex. 1005 ¶ 310 (relying on Ex. 1007, 11:26–36, 11:45–55). Dr. Tamassia further testifies that “[t]o initiate the secure IP tunnel, the trusted third-party network device will look-up the IP address of the corresponding second network device.” *Id.* (citing Ex. 1007, 9:6–8, 11:26–36). Paragraph 310 of Dr. Tamassia’s testimony is cited in the Petition as support that Beser teaches a request to look up an IP address. *See* Pet. 33.

We have reviewed the Monroe Declaration for testimony relevant to whether Beser teaches a request to look up an IP address. Dr. Monroe’s opinion based on the tunneling association taught by Beser is that “[o]ne of ordinary skill in the art would not understand this request (*even containing a ‘unique identifier’*) to be a ‘request to look up an internet protocol (IP) address of the second network device.’” Ex. 2016 ¶¶ 28 (relying on Ex. 1007, 7:65–67, 8:1–3) (emphasis added). This testimony of Dr. Monroe emphasizes the fact that a “unique identifier” is included in the tunneling request. That same “unique identifier” contained in a database forms a basis for Dr. Tamassia’s opinion that the tunneling request of Beser is a request to look up an IP address. *See* Ex. 1005 ¶ 310. For this and other reasons addressed below, we credit the Tamassia Declaration testimony that Beser’s request to initiate a tunneling connection is a request to look up an IP

address. In reaching our conclusion, we focus on what a person of ordinary skill in the art would understand from Beser and not the difference in terminology between a tunneling request and an IP address look up.

We also agree with Petitioner that Beser teaches “the trusted-third-party network device will look up and return to the first network device a public IP address for the second network device and a private IP address for the terminating device.” Pet. 34 (citing Ex. 1007, 11:26–36, 12:28–32, 14:19–27, 17:42–49; Ex. 1005 ¶¶ 310, 339). With respect to public IP addresses, Beser teaches “[a] public IP 58 address for a second network device 16 is associated with the unique identifier for the terminating telephony device 26.” Ex. 1007, 11:26–28. This teaching is relied on by Dr. Tamassia to reach his conclusion. *See* Ex. 1005 ¶ 310. With respect to private IP address, Beser teaches that “on the first network device 14 is recorded the first private IP 58 address for the originating telephony device 24, and on the second network device 16 is recorded the second private IP 58 address for the terminating telephony device 26.” Ex. 1007, 12:28–32. With respect to the role of the trusted-third-party device, Beser teaches:

The trusted-third-party network device 30 constructs a fourth IP 58 packet 168 with the public IP 58 address of the trusted-third-party network device 30 in the source address field 88 and the public IP 58 address of the first network device 14 in the destination address field 90. Included in the payload field 84 of the fourth IP 58 packet 168 is the second private IP 58 address and the public IP 58 address of the second network device 16. The fourth IP 58 packet 168 is sent to the first network device 14 on the public network 12. The first network device 14 receives the fourth IP 58 packet 168, examines the payload 84, and determines that it includes both the second private IP 58 address that has been assigned to the terminating end of the

tunneling association 26 and the public IP 58 address of the second network device 16.

Ex. 1007, 14:19–33. This teaching is relied on by Dr. Tamassia to reach his conclusion that Beser teaches requesting an IP look up. *See* Ex. 1005 ¶ 339.

The preceding discussion of what Petitioner shows at page 34 of the Petition, which Patent Owner disputes at pages 22 and 23 of the Response, is addressed in Paragraph 33 of the Monroe Declaration. Ex. 2016 ¶ 33 (citing Pet. 34). Other than a conclusory denial of Petitioner’s assertion, Dr. Monroe does not respond to or testify about any of the passages from Beser relied upon by Petitioner and reproduced above. Rather, Dr. Monroe focuses on one isolated disclosure in Beser and concludes “one of ordinary skill in the art would have understood that the negotiation does not involve looking up any IP address, but rather involves *assignment* of a first private network address to the originating device and a second private network address to the terminating device.” *Id.* (citing Ex. 1007, 12:2–4).

Again, the difference in terminology between “assignment” and “look up” is not persuasive. We agree with Petitioner that “even if second network device 16 ‘assigns’ the IP address to terminating device 2[6], the trusted device 30 ‘looks up’ the IP address when it sends a message to network device 16 requesting a private IP address.” Pet. Reply 11–12 (citing Ex. 1007, Fig. 9 (packets 164 & 166), 13:34–48, 13:66–14:18; Pet. 20–21, 38). Second, as Petitioner points out, what actually occurs in Beser is that “[t]he second private IP 58 address is selected from a second pool of private IP 58 addresses on the second network device 16.” Ex. 1007, 13:49–51; *see also* PO Resp. 11 (citing Pet. 20).

Finally, we note that neither claim 1 nor 21 specify how the IP address is requested, or what device looks it up. All the claim language requires is “a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device.” As such, it is of no import that Beser’s trusted device 30 looks up the public IP address of second network device 16 instead of terminating device 26. *See* PO Resp. 23; Pet. Reply 10–11.

In summary, Beser teaches that the trusted-third-party network device receives a request to initiate a tunneling association and uses the unique identifier in the request to look up an Internet Protocol (IP) address in the database of unique identifiers. Ex. 1007, 11:26–36, 11:45–55. Public IP addresses for second network device 16 are associated with the unique identifier for terminating telephony device 26. *Id.* at 11:26–28. Private IP addresses are recorded on the first network device 14 for the originating telephony device 24 and on the second network device 16 for the terminating telephony device 26. *Id.* at 12:28–32. The trusted-third-party device sends packets including Internet Protocol (IP) addresses between the first and second network devices 14 and 16. Ex. 1007, 14:19–33. The first network device determines that second private IP 58 address that has been assigned to the terminating end of the tunneling association 26 and the public IP 58 address of the second network device 16. *Id.*

We, therefore, conclude that Petitioner shows by a preponderance of evidence that Beser discloses sending the claimed request to look up an Internet Protocol (IP) address.

b. Intercepting

Patent Owner's second argument is that Beser does not teach the request to look up an Internet Protocol (IP) address is "intercepted." PO Resp. 23–27. As discussed in detail above, Petitioner alleges the tunneling request in Beser is "'intercepted' by each of the first network device and the trusted-third-party network device because they each receive 'a request pertaining to a first entity at another entity.'" Pet. 33 (citing Ex. 1007, 8:21–47; Ex. 1005 ¶ 69).

Patent Owner responds that the tunneling request cannot be "intercepted" by first network device 14 or trusted-third-party network device 30, because in Beser's system, tunneling requests "always go to, and are always intended to go to the first network device." PO Resp. 24. Patent Owner contends that Petitioner's expert, Dr. Tamassia, required an element of intent in the construction of "interception of a DNS request" and Beser does not satisfy the requirement. *Id.* (citing Ex. 2016 ¶ 36; Ex. 2015, 80:3–13).

Patent Owner's contentions are not persuasive. As set forth above, the "interception of a request to look up an Internet Protocol (IP) address" does not include an element of intent. Furthermore, no party proposed an "intent" element in the construction of the "interception" limitation in this proceeding. Pet. 10; PO Resp. 11 (listing both parties' claim construction proposals).

In any event, as Petitioner explains, regardless of what any potential "intent" element of "interception of a request to look up an Internet Protocol (IP) address" entails, in the '705 patent, all requests are intended to go to the proxy DNS (i.e., not another entity), which the Specification characterizes as

intercept[ing] all DNS lookup functions.” Pet. Reply 13 (citing Ex. 1001, 40:1–3). “The ’705 patent thus provides that DNS proxy 2610 ‘intercepts’” lookup functions, even though the DNS proxy receives every single lookup request sent by the client.” *Id.* Dr. Monroe agreed that the DNS proxy in the ’705 patent receives every DNS request and that the system is designed, “pre-established” to intercept every DNS request. Ex. 1066, 55:8–20.

Based on the preceding, Petitioner urges us to reject “Patent Owner’s arguments that Beser cannot show an ‘intercepting’ because it is designed such that IP tunnel requests are received by network device 14 and trusted device 30.” Pet. Reply 13. We agree. The record shows that Beser’s first network device 14 and trusted-third-party device 30 operate just like the disclosed proxy DNS in the context of intercepting requests. In other words, as explained above in the claim construction section, the ’705 patent treats “intercepting” by the intermediate proxy DNS as “receiving” a request to look up an address for another entity (e.g., a target or end device), and both parties agree “receiving” constitutes “intercepting.” *See*, Tr. 31:8–32:23 (Patent Owner counsel stating that the ’705 patent does not specify how interception occurs), Tr. 37:12–21 (Patent Owner counsel stating that if we adopted Patent Owner’s construction of “interception of DNS request,” Beser does not pose a patentability problem because it doesn’t disclose encryption—not that it doesn’t receive the DNS request).

c. Combination of Beser and RFC 2401

As noted above, Petitioner provides several reasons explaining why an artisan of ordinary skill would have used end-to-end encryption, as disclosed and suggested by RFC 2401, in Beser’s similar network system, for example, to provide enhanced data security and anonymity in networks

having similar topology. Pet. 26–30. Petitioner also notes that Beser itself suggests the encryption of data using the IPsec protocol, the same encryption protocol that RFC 2401 defines. *See* Pet. 27–31; Ex. 1007, 1:54–56; Ex. 1008, 4, 7, 10. Petitioner notes that RFC 2401 in its “case 3” example “shows precisely the same network topology as Beser, with one tunnel between two security gateways such as edge routers, and another tunnel between the two end devices.” Pet. 28 (comparing Ex. 1008, 25 with Ex. 1007, Fig. 1; Ex. 1005 ¶¶ 396–397).

In response, Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner. PO Resp. 27–33. Patent Owner contends that Beser teaches away from encryption. According to Patent Owner, Beser explains that prior art systems typically addressed Internet security either by encrypting the information inside packets prior to transmission or by using address translation. PO Resp. 27 (citing Ex. 1007, 1:54–2:35). Beser acknowledges that both solutions have disadvantages. For example, encryption can “require a great deal of computing power to encrypt or decrypt the IP packets on the fly.” *Id.* (citing Ex. 1007, 1:62–63). Patent Owner contends that Beser notes the problems with allocating more computing power to encryption, such as “jitter, delay, or the loss of some packets,” and, therefore, “dismisses the idea of encryption entirely, noting that the ‘expense of added computer power might also dampen the customer’s desire to invest in VoIP equipment’ at all.” *Id.* at 28 (citing Ex. 1007, 1:65–67).

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

By hiding the identities of the network devices in this manner, *Beser* touts that its method is able to *increase* communication security *without increasing* computational burden. ([Ex. 1007,] 2:43–3:14.) Thus, one of ordinary skill in the art would have understood that *Beser* is directed to providing a method for securing communications *other than* encryption. (See Ex. 2016 at ¶ 45.)

PO Resp. 29.

Patent Owner explains that “*Beser* also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, *Beser* eschews encryption in favor of hiding the identities within the tunnel.” PO Resp. 31. According to Patent Owner, the purpose of the encryption in *Beser* “is simply to hide address information on the public network prior to *Beser*’s tunnel establishment, once the tunnel is created, the originating and terminating device information is hidden and encryption would not only be redundant, it would contravene *Beser*’s express objective of increasing security without increasing computational burden.” *Id.* at 31 (citing Ex. 2016 ¶ 47).

We do not agree with Patent Owner’s description of what a person of ordinary skill would have understood from *Beser*’s disclosure. Although *Beser* recognizes that the use of encryption may cause challenges, *Beser* also suggests that such problems may be overcome by providing more computer power and/or less quality. See Ex. 1007, 1:60–67. For example, *Beser* teaches that an “increased *strain on computer power* [i.e., as opposed to increased computer power] may result in jitter, delay, or the loss of some packets.” *Id.* at 1:63–64. Moreover, *Beser* never states that its technique of hiding addresses is intended as replacing, as opposed to supplementing,

known security techniques such as encryption. In fact, Beser implies that a good system will allow multiple types of security solutions to be used at the same time, by characterizing some prior art systems as creating “*security problems by preventing certain types of encryption from being used.*” Ex. 1007, 2:23–24 (emphasis added).

We credit testimony by Dr. Tamassia stating that “[a] person of ordinary skill in the art reading *Beser* in February 2000 would also have understood that encryption should ordinarily be used even in high data volume applications, if possible” and that such a person “would recognize that the concerns expressed in *Beser* . . . can be easily resolved by simply using more powerful equipment.” Ex. 1005 ¶¶ 389–390. Dr. Tamassia’s conclusion is supported by explanation and citation to the record. *Id.* ¶¶ 384–399 (citing Ex. 1007, *passim*; Ex. 1008, 25). Dr. Monroe’s testimony does not persuade us to the contrary as it largely echoes Patent Owner’s unpersuasive attorney argument. *Compare* Ex. 2016 ¶¶ 40–48 *with* PO Resp. 27–33. We find that Beser at most mildly criticizes (tempered by an implied solution) a specific type of tunneling that employs encapsulation, encryption, and VoIP packets—i.e., “due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.” Ex. 1007, 2:15–17. In other words, Beser at least suggests that with adequate power or typical data transmissions, a tunnel (a VPN according to Beser) and encryption would be appropriate for providing security. Therefore, we find that Beser does not discourage encrypting data to make it secure; rather, Beser provides a solution for providing anonymity by using a tunnel technique with or without encryption of data, and if necessary, increasing computer power as needed.

Thus, notwithstanding Patent Owner's arguments, a preponderance of evidence supports a finding that a person of ordinary skill reading Beser at the relevant time would have understood that encryption should ordinarily be used to protect the contents of the communications in an IP tunnel.

Petitioner, thus, establishes by a preponderance of the evidence that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with those of Beser to encrypt data in order to enhance data security in a tunnel that provides anonymity, based on a determination that a requested target device would have been available for a secure communication.

We determine Petitioner has shown by a preponderance of the evidence that claims 1 and 21 would have been obvious over Beser combined with RFC 2401.

H. Claims 3, 10, and 25

Petitioner asserts that the combination of Beser and RFC 2401 teaches each of the limitations of claims 3, 10, and 25. Pet. 43–44. Claims 3 and 10 depend directly or indirectly from claim 1. Claim 25 depends from claim 21. The single limitation in all three claims is “wherein the domain name is a secure domain name.” As discussed above, we construed “secure domain name” to mean “a name that corresponds to a secure computer network address.”

Petitioner argues Beser shows that the unique identifier can be a domain name, and that the IP tunnel between the end devices, each with a private IP address, to transmit data between each other across a public network. Pet. 43–44 (citing Ex. 1007, 7:64–8:20, 10:38–41, 10:55–11:5, 10:66–11:2; Ex. 1005 ¶¶ 308, 319, 330, 333). Petitioner concludes Beser

thus shows a “secure domain name” because the “unique identifier can be a name that corresponds to a secure computer network address (i.e., the private IP address of the terminating end device).” *Id.* at 44 (citing Ex. 1005 ¶¶ 319, 323–325). Petitioner’s additional showing regarding Beser teaching a secure domain name is that the third-party network device can require “encryption or authentication” before initiating a tunneling association. *Id.* (citing Ex. 1007, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 391–392). Petitioner relies on the testimony of Dr. Tamassia that “[t]he originating end device must authenticate before it can obtain the private IP address of the terminating end device.” *Id.* (citing Ex. 1005 ¶ 391).

Patent Owner opposes Petitioner’s showing by relying on its proposed construction of “secure domain name” as meaning a “*non-standard domain name* that corresponds to a secure computer network address and *cannot be resolved by a conventional domain name service (DNS)*.” PO Resp. 33. More specifically, Patent Owner argues “Beser does not disclose any non-standard domain names that cannot be resolved by a conventional DNS.” *Id.* (citing Ex. 1007, 10:38–41; Ex. 2016 ¶ 49).

As discussed above in II.A.2., our construction of “secure domain name” rejected Patent Owner’s argument that a secure domain name is a “non-standard domain name.” Patent Owner does not argue that claims 3, 10, and 25 would not have been obvious under the final construction of “secure domain name.” Even were we to adopt Patent Owner’s construction, as Petitioner notes, Patent Owner has previously argued a non-standard domain name can include a telephone number, such as disclosed in Beser. *See* Pet. Reply 16 (citing File History of U.S. Patent No. 8,051,181, 9 (Ex. 1069); Pet. 18, 43 (citing Ex. 1007, 10:38–41)). Also, Beser’s domain

names are not resolved solely by a conventional DNS process, but rather include a negotiation process. *See* Ex. 1009, Figs. 4–5. Beser also makes it clear that it does not restrict names to conventional domain names and services: “many more unique identifiers and trusted-third-party network devices are possible.” *Id.* at 11:57–58. Therefore, Beser implies or at least suggests using a non-standard domain name associated with a secure device that satisfies Patent Owner’s construction or Petitioner’s construction. We determine Petitioner has shown by a preponderance of the evidence that claims 3, 10, and 25 would have been obvious over Beser combined with RFC 2401.

I. Claims 4 and 26

Claim 4 depends from method claim 1 and recites additionally that “the encrypted communications channel is a broadband connection.” Claim 26 depends from claim 21 and repeats the “broadband connection” limitation in the context of system claim 21. Petitioner asserts Beser teaches that “the first and second network devices can be cable modems or cable modem termination systems that communicate via cable television networks” and the data transmitted is “necessarily transmitted over a broadband connection.” Pet. 44–45 (citing Ex. 1007, 4:30–36, Ex. 1005 ¶¶ 80, 294, 297).

Patent Owner alleges the Petition relies on inherency in arguing “[d]ata transmitted over a cable television network is *necessarily* transmitted over a broadband connection.” PO Resp. 34 (citing Pet. 44–45). Patent Owner argues evidence that data is necessarily transmitted over a broadband connection is insufficient because Dr. Tamassia does not disclose the

“underlying facts or data” under 37 C.F.R. § 41.65(a) to support the inherency proposition. *Id.* (citing Ex. 1005 ¶ 80).

Petitioner argues that “broadband connection” is shown by use of a cable modem and not just “cable television communications.” Pet. Reply 17 (citing Pet. 44–45). Petitioner argues the Tamassia Declaration at paragraph 80 discusses the terms “modulated” and “unmodulated,” i.e., “[e]xamples of modulated signals include data transmitted via a modem (i.e., a “modulator-demodulator” device) and data transmitted via a cellular or cable network.” *Id.* (citing Ex. 1005 ¶ 80). Petitioner concludes “a *cable modem* over [sic] to communicate over a cable television network necessarily used a broadband connection because the modem allows for multiple channels over the link.” *Id.* (citing Pet. 44).

We agree with Petitioner. The ’705 patent defines a broadband communication medium as “separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link.” Ex. 1007, 34:51–55. We credit Dr. Tamassia’s testimony above that “examples of modulated signals include data transmitted via modem and data transmitted via cellular or cable network.” *See* Pet. 45 (citing Ex. 1005 ¶ 80). Accordingly, we determine Dr. Tamassia discloses the necessary facts he relies on to give the opinions testified to as required by 37 C.F.R. § 41.65(a). Finally, the Petition points to Beser, which says that it can use cable modems over cable networks. *Id.* at 44 (citing Ex 1007, 4:30–36). None of the preceding requires an inherency analysis and we determine it would have been obvious to the person of ordinary skill in the art to use a “broadband connection” with an “encrypted communications channel.” We determine that Petitioner has shown by a preponderance of the evidence that

claims 4 and 26 would have been obvious over Beser combined with RFC 2401.

J. Claims 14 and 31

Claim 14 depends from method claim 1 and recites additionally “wherein the target device is a server.” Claim 31 depends from claim 21 and repeats the “server” limitation in the context of system claim 21. Petitioner argues Beser describes various originating and terminating end devices, including Web-TV sets and decoders, interactive vide-game players, or personal computers running multimedia applications. Pet. 46 (citing Ex. 1007, 4:43–54; *see also* 4:14–18). Petitioner notes that Beser describes that the terminating end device can be a domain name. *Id.* at 46–47 (citing Ex. 1007, 10:37–41, 10:55–11:5). Petitioner concludes a person of ordinary skill in the art “would understand that a Web-TV device or a multimedia application would be used by connecting to and downloading content from a server.” *Id.* (citing Ex. 1005 ¶ 289).

First, Patent Owner contends that Petitioner relies on inherency to meet the limitation and does not provide evidence beyond that “the terminating device 26 (the alleged target device) *can connect* to a server,” not that it does connect to a server. PO Resp. 35. Patent Owner quotes Petitioner’s expert testimony that Web-TV and multimedia applications “*could* be used to connect to and download[] from a server.” *Id.* at 35–36 (citing Ex. 1005 ¶ 289). Patent Owner also argues that Beser’s disclosure of domain names does not support the existence of a server because Petitioner has “repeatedly contended, this ‘name server’ is the trusted-third-party network device—not the client or target device.” *Id.* at 36 (citing Pet. 35).

We find that Petitioner does not argue inherency but what a person of ordinary skill would understand from the disclosure of Beser. Petitioner argues a Web-TV streams content from a server. Pet. 46–47 (citing Ex. 1005 ¶289). We agree with Petitioner that “[a] person of ordinary skill in the art would have understood that where originating device 24 is a Web-TV, terminating device 26 is a Web-TV *server* that sends television content to the client.” Pet. Reply 18 (citing Ex. 1005 ¶ 289). Further, Dr. Tamassia’s opinion is supported by specific reference to what is shown in Beser. *See* Ex. 1005 ¶ 289 (relying on Ex. 1007, 4:47–49)). We also agree with Petitioner’s contention that Beser discloses “other types of network devices” for end devices, and specifically discloses personal computers, Web TV sets, decoders, etc., “which would suggest to a person of ordinary skill in the art” that that terminating end devices could be servers with domain names for providing services or data to other devices. *See* Pet. 46 (citing Ex. 1005 ¶¶ 122–128; Ex. 1007, 10:39–41, 10:55–11:5).

We determine that Petitioner has shown by a preponderance of the evidence that claims 14 and 31 would have been obvious over Beser combined with RFC 2401.

K. Claims 18–20 and 22–24

Claims 18 and 22 depend from claims 1 and 21 respectively and recite that “the encrypted communications channel supports a plurality of services.” Claims 19 and 20 and claims 23 and 24 further depend directly or indirectly from claims 18 and 22, respectively.

The Petition alleges the tunnel disclosed in Beser is the claimed “communications channel.” *See* Pet. 30–31 (claims 1 and 21). Petitioner contends that “the IP tunnel can be implemented over a variety of networks,

such as the Internet, an intranet, Local Area Networks and cable television networks.” *Id.* at 48–49 (citing Ex. 1007, 4: 30–42; Ex. 1005 ¶¶ 294–298). Concerning the claimed “services,” Petitioner cites to Beser’s teaching that the data sent over an IP tunnel can include data for facsimile or audio applications, data for “Web-TV sets,” VoIP data, and video conference data for the “H.323 protocol,” a protocol used for multimedia communications include voice. Pet. 49 (citing Ex. 1007, 4:50–52, 4:47–50, 9:67–10:2; Ex. 1005 ¶¶ 286–298).

Patent Owner observes the Petition alleges that “Beser’s underlying network (not the tunnel) has the capability of supporting a plurality of services.” PO Resp. 21 (citing Pet. 48–49). Patent Owner contends that Beser’s network is not the same as the tunnel. *Id.* at 37 (citing Ex. 2016 ¶ 52). Patent Owner argues “a multi-service-capable network does not necessitate that Beser’s tunnel also supports a plurality of services. *Id.* at 38.

We find that Beser clearly states the IP tunnel may be implemented on various networks “such as the Internet, an intranet, Local Area Networks and cable television networks.” Pet. 48–49 (citing Ex. 1007, 4: 30–42; Ex. 1005 ¶¶ 294–298). Indeed, Patent Owner does not dispute that Beser discloses these underlying networks provide services. *Id.* at 49 (citing Ex. 1007, 4:50–52, 4:47–50, 9:67–10:2; Ex. 1005 ¶¶ 286–298).

Patent Owner’s argument presupposes that the services are simultaneously supported. We agree with Petitioner that the claim language includes no such requirement. *See* Pet. Reply 18.

We determine that Petitioner has not shown by a preponderance of the evidence that claims 14 and 31 would have been obvious over Beser combined with RFC 2401.

L. Claims 2, 6–9, 12–13, 15–17, 28–30, and 32–34

Petitioner asserts that the combination of Beser and RFC 2401 teaches each of the limitations of claims 2, 6–9, 12–13, 15–17, 28–30, and 32–34. We have reviewed Petitioner’s evidence regarding these claims. *See* Pet. 41–48. According to Petitioner, Beser suggests each of the limitations added to independent claims 1 and 21 by the challenged dependent claims 2, 6–9, 12–13, 15–17, 28–30, and 32–34. *Id.* at 41, 45–48.

Claims 2 and 9 recite that providing the provisioning information “is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an [sic] network address lookup.” Petitioner asserts that a person of ordinary skill in the art would have considered the limitation obvious because it would have been obvious to make a “determination” as to whether the terminating end device accepts communications via an encrypted communications channel. Pet. 42. Petitioner’s next step of its showing is that “the trusted third-party network device negotiates with the first and second network devices to establish a private IP tunnel.” *Id.* (citing Ex. 1007, 9:6–11, 9:26–30, 11:9–44; Ex. 1005 ¶¶ 330, 333, 335–340. Once the unique identifier is associated, private IP addresses are negotiated. *Id.* at 43 (citing Ex. 1007, 9:6–28, Fig. 4; Ex. 1005 ¶¶ 330, 333, 335–340).

In its Response, Patent Owner does not make specific arguments directed to the challenged dependent claims and instead argues that “*Beser* and RFC 2401 do not render obvious claims 2, 6–9, 12–13, 15–17, 28–30, and 32–34 for at least the reasons discussed above for independent claims 1 and 21, from which they depend.” PO Resp. 38.

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 and adopt Petitioner's analysis. Thus, we determine that Petitioner has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found dependent claims 2, 6–9, 12–13, 15–17, 28–30, and 32–34 obvious over Beser and RFC 2401.

OBVIOUSNESS-BESER, RFC 2401 AND BRAND

Petitioner alleges claims 5, 11, and 27 would have been obvious over Beser, RFC 2401, and Brand. Pet. 51–52. Petitioner's evidence includes testimony from Dr. Tamassia. Ex. 1005 ¶¶ 404–408, 414–417, 423.

M. Overview of Brand

Brand discloses that networks can be categorized into two basic networks based on the type of bandwidth used in the network: “broadband systems and baseband systems.” Ex. 1012, 1:26–29; Ex. 1005 ¶¶ 406–407. Brand also discloses that baseband networks are “unmodulated.” *Id.* at 1:31–33.

N. Claims 5, 11, and 27

Claims 5 and 27 depend respectively from claims 1 and 21 and both recite “wherein the encrypted communications channel is an unmodulated transmission link.” Claim 11 depends from claim 8 and recites the same limitation as do claims 5 and 27. We have reviewed Petitioner's evidence regarding these claims. See Pet. 51–52.

Petitioner argues Beser discloses “backbone” networks including both broadband and baseband systems. Pet. 51 (citing Ex. 1007, 4:15–36; Ex. 1012, 1:26–29; Ex. 1005 ¶ 406). Brand is cited as teaching that baseband

networks are “unmodulated.” *Id.* (citing Ex. 1012, 1:31–33; Ex. 1005 ¶ 406). Petitioner concludes, “it would have been obvious for a person of ordinary skill in the art to choose to use a baseband network to implement Beser’s public network connection because a baseband network is one of the two basic types of networks.” *Id.* (citing Ex. 1005 ¶ 417; Ex. 1012, 1:26–29).

Petitioner asserts a person of ordinary skill would have combined Beser, RFC 2401, and Brand based on the rationale relating to Beser and RFC 2401. *Id.* at 52. The rationale for additionally combining Brand includes that “Brand is directed to two different types of networks [and,] it would have been advantageous for the combined system of Beser and RFC 2401 (offering encrypted end-to-end communication) to work on as many network types as possible.” *Id.* (citing Ex. 1005 ¶ 423).

In its Response, Patent Owner does not make specific arguments directed to the challenged dependent claims and instead argues that “*Beser*, RFC 2401, and *Brand* do not render obvious claims 5, 11, and 27 for at least the reasons discussed above for independent claims 1 and 21, from which they depend.” PO Resp. 38.

We have reviewed both parties’ arguments and supporting evidence, including the disclosure of both references and the testimony of Dr. Tamassia and we agree with and adopt Petitioner’s analysis. Thus, we determine that Petitioner has shown, by a preponderance of the evidence, that a person of ordinary skill in the art would have found dependent claims 5, 11, and 27 obvious over Beser, RFC 2401, and Brand.

O. Patent Owner's Motion to Exclude

Patent Owner seeks to exclude Exhibits 1001, 1002, 1009–35, 1037–41, 1043–48, 1060, 1063–65, 1068, 1069, and portions of 1005. Paper 36, 1. As movant, Patent Owner has the burden of proof to establish that it is entitled to the requested relief. *See* 37 C.F.R. § 42.20(c). For the reasons stated below, Patent Owner's Motion to Exclude is *dismissed*.

1. Exhibits 1060 and 1063–65

Patent Owner seeks to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 35, 2. Exhibit 1060 is a declaration originally submitted in litigation before the International Trade Commission. Ex. 1060. It contains testimony from Sandy Ginoza, a representative of IETF, in support of Petitioner's contention that RFC 2401 qualifies as a printed publication as of November 1998. *Id.* Exhibit 1063 is a "transcript of Ms. Ginoza's February 8, 2013 deposition that was taken as part of the ITC action." Paper 35, 2 (quoting Paper 17, 5–6). Exhibits 1064 and 1065 are both magazine articles dated 1999 that relate to this same issue. Paper 17, 5–7. All four exhibits were entered into the record upon Petitioner's Motion to Submit Supplemental Information Pursuant to 37 C.F.R. § 42.123(a). Paper 17; Paper 21.

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.

2. Exhibits 1003, 1004, 1009–1011, 1013–1035, 1037–1041, 1043–1048, and 1068

Patent Owner seeks to exclude the above listed exhibits as lacking relevance. Paper 35, 3. Because we do not rely on any evidence subject to

the motion, the listed exhibits are irrelevant and we dismiss this request as moot.

3. Portions of Exhibit 1005

Patent Owner seeks to exclude portions of Dr. Tamassia's testimony in Exhibit 1005 as lacking relevance because they relate to Aventail. Paper 35, 4. Aventail is a reference relied on by Petitioner in IPR2015-00811 but not here. Because we do not rely on any paragraphs of Exhibit 1005 subject to the motion, the cited portions of Dr. Tamassia's testimony are irrelevant and we dismiss this request as moot.

III. ORDER

For the reasons given, it is:

ORDERED that claims 1–34 of U.S. Patent No. 8,868,705 B2 have been shown by a preponderance of the evidence to be unpatentable;

FURTHER ORDER that Patent Owner's Motion to Exclude (Paper 36) is *dismissed* as moot; 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.

IPR2015-00810
Patent 8,868,705 B2

PETITIONER:

Jeffrey P. Kushan
Scott Border
Thomas A. Broughan III
SIDLEY AUSTIN LLP

jkushan@sidley.com
sborder@sidley.com
tbroughan@sidley.com
IPRNotices@sidley.com

PATENT OWNER:

Joseph E. Palys
Naveen Modi
Daniel Zeilberger
Chetan Bansal
PAUL HASTINGS LLP

josephpalys@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com
chetanbansal@paulhastings.com

Jason E. Stach
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Jason.stach@finnegan.com