Trials@uspto.gov
571-272-7822

Paper 35
Date: August 24, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00481
Patent 7,188,180 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge*.

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

I. BACKGROUND

Apple Incorporated ("Petitioner") filed a revised Petition requesting *inter partes* review of claims 1, 4, 6, 10, 12–15, 17, 20, 22, 26, 28–31, 33, 35, and 37 of U.S. Patent No. 7,188,180 B2 ("the '180 patent," Ex. 1001) pursuant to 35 U.S.C. §§ 311–319. Paper 1 ("Pet."). The Board instituted an *inter partes* review of claims 1, 4, 6, 10, 12–15, 17, 20, 22, 26, 28–31, 33, 35, and 37. Paper 11 ("Inst. Dec.").

Prior to institution, VirnetX Incorporated ("Patent Owner") filed a Patent Owner Preliminary Response (Paper 7) ("Prelim. Resp."), and after institution, filed a Patent Owner Response (Paper 20) ("PO Resp."). Petitioner then filed a Reply (Paper 24) ("Pet. Reply"). An oral hearing occurred on June 2, 2015 and a transcription of same is in the record. Paper 34 ("Tr.").

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1, 4, 6, 10, 12–15, 17, 20, 22, 26, 28–31, 33, 35, and 37 of the '180 patent are unpatentable.

A. The '180 Patent (Ex. 1001)

The '180 patent Specification describes a system for establishing a secure communication link between a first computer and a second computer over a computer network. Ex. 1001, 6:41–44, 49:57–59, Abstract. The user obtains a universal resource locator (URL) for a secure top-level domain name by querying a secure domain name service (SDNS) that contains a cross-reference database of secure domain names and corresponding secure network addresses. *Id*. at 51:32–35, 52:6–8. When the user queries the

secure domain name service for a secure computer network address, the secure domain name service determines the particular secure computer network address and returns the network address corresponding to the request. *Id*. at 39:59–62:3, 52:22–26.

In one embodiment, a secure domain name server, "SDNS 3313, determines the particular secure network address based on the user's identity and the user's subscription level." *Id*. at 52:24–26. "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name." *Id.* at 52:4–8.

The '180 patent Specification also describes creating a secure communication link in the form of a virtual private network ("VPN") link. One preferable "VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence." *Id.* at 51:52–55. The '180 patent Specification refers to this technique and similar techniques as an "IP address hopping regime" or "particular information hopping technique." *Id.* at 51:56, 52:1–2.

B. Illustrative Claim

According to Patent Owner, and as the record reflects, independent claims 1, 17, and 33 "recite similar features." PO Resp. 26. Therefore, this Final Written Decision focuses on claim 1, unless otherwise noted. Claim 1 follows:

> 1. A method for accessing a secure computer network address, comprising steps of:
>
> receiving a secure domain name;

> sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
>
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
>
> sending an access request message to the secure computer network address using a virtual private network communication link.

C. Cited Prior Art

Provino US 6,557,037 B1 Apr. 29, 2003 (Ex. 1003)

Dave Kosiur, *Building and Managing Private Networks* (Sept. 1, 1998) (Ex. 1006, "Kosiur").

D. Instituted Grounds of Unpatentability

References	**Basis**	**Claims Challenged**
Provino	§ 102	1, 10, 12–15, 17, 26, 28–31, and 33
Provino and Kosiur	§ 103	4, 6, 20, 22, 35, and 37

E. Claim Construction

In an *inter partes* review, the Board interprets claim terms in an unexpired patent according to the broadest reasonable construction in light of the specification of the patent in which they appear. *In re Cuozzo Speed Techs., LLC*, No. 2014-1301, 2015 WL 4097949, at *6 (Fed. Cir. July 8, 2015); 37 C.F.R. § 42.100(b). Under that standard, claims must be construed according to their ordinary and customary meaning, in view of the specification, as would be understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). A "lexicographer" who redefines a claim term to

have an "uncommon meaning[]"or "uncommon definition" must do so with "reasonable clarity, deliberateness, and precision." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citation omitted).

Recently, the Federal Circuit indicated that even for non-expired patents that return to the PTO, prosecution history may be an important component of intrinsic evidence in construing claims (notwithstanding that Patent Owner may amend the claims and a broadest reasonable construction standard applies).[1] *See Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 977 (Fed. Cir. 2014) ("In claim construction, this court gives primacy to the language of the claims, followed by the specification. Additionally, the prosecution history, while not literally within the patent document, serves as intrinsic evidence for purposes of claim construction. This remains true in construing patent claims before the PTO.") (citing *In re Morris*, 127 F.3d 1048, 1056 (Fed. Cir. 1997)); *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015) ("The PTO should also consult the patent's prosecution history in proceedings in which the patent has been brought back to the agency for a second review.") (citing *Tempo Lighting*, 742 F.3d

[1] For district court litigation and for expired patents that return to the PTO, claims cannot be amended. Those claims must be construed using their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the invention, in light of the language of the claims, the specification, and the prosecution history of record. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–17 (Fed. Cir. 2005) (en banc); *In re Rambus*, 694 F.3d 42, 46 (Fed. Cir. 2012) ("[T]he Board's review of the claims of an expired patent is similar to that of a district court's review."); *Cuozzo*, 2015 WL 4097949, at *6 n.6 ("The claims of an expired patent are the one exception where the broadest reasonable interpretation is not used because the patentee is unable to amend the claims.") (citing *In re Rambus, Inc.*, 753 F.3d 1253, 1256 (Fed. Cir. 2014)).

at 977); *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1349 (Fed. Cir. 2004) ("[T]he prosecution history of one patent is relevant to an understanding of the scope of a common term in a second patent stemming from the same parent application."). On the other hand, in *Tempo Lighting*, 742 F.3d at 978, the "court also observes that the PTO is under no obligation to accept a claim construction proffered as a prosecution history disclaimer, which generally only binds the patent owner."

Although disclaimers or lexicographic definitions in a specification may be express, they need not be. *Compare In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004) ("Absent claim language carrying a narrow meaning, the PTO should only limit the claim based on the specification or prosecution history *when those sources expressly disclaim* the broader definition.") (emphasis added), *with Bell Atl. Network Servs., Inc. v. Covad Commc'ns Grp., Inc.*, 262 F.3d 1258, 1268 (Fed. Cir. 2001) ("[A] claim term may be clearly redefined without an explicit statement of redefinition. . . . In other words, the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents.") (citations and internal quotation marks omitted), *and Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("The specification acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication.").

In any case, prosecution history disclaimers, like uncommon or lexicographic meanings, must be clear and unambiguous: "[W]hile the prosecution history can inform whether the inventor limited the claim scope in the course of prosecution, it often produces ambiguities created by ongoing negotiations between the inventor and the PTO. Therefore, the

doctrine of prosecution disclaimer only applies to unambiguous disavowals." *Grober v. Mako Prods., Inc*., 686 F.3d 1335, 1341 (Fed. Cir. 2012) (citing *Abbott Labs. v. Sandoz, Inc*., 566 F.3d 1282, 1289 (Fed. Cir. 2009)). A "heavy presumption" exists in favor of the ordinary meaning of claim language. *Bell Atl. Network Servs., Inc.*, 262 F.3d at 1268. To overcome this presumption, the patentee must "clearly set forth" and "clearly redefine" a claim term away from its ordinary meaning. *Id.* The disavowal must be "unmistakable" and "unambiguous." *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1322 (Fed. Cir. 2013). This standard is "exacting." *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1366 (Fed. Cir. 2012).

Independent claims 1, 17, and 33 recite the following terms:

1. Virtual Private Network (VPN) Communication Link

In a related case, on a similar record, the Board determined that a "VPN communication link" is "a secure communication link that includes a portion of a public network." *See Apple Inc. v. VirnetX Inc.*, Case IPR2014-00237, slip. op. at 5–9 (PTAB May 11, 2015) (Paper 41) (the "'237IPR"). For consistency with Figure 33 of the '180 patent (as discussed below) and the '237IPR, although it is not material to the issue here, we add the requirement that the VPN communication link includes a portion of a public network (which otherwise is insecure). *See* note 3 *infra*. (In essence, a "virtual private" link, uses, at least in part, a public link.)

In this case, we previously construed the term "virtual private network communication link" to mean "a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address

hopping." Inst. Dec. 7 (i.e., generally, tracking the construction of a secure communication link but without the public network requirement, *see* '237IPR, Paper 41, 8–10).[2] Patent Owner "disagrees with this construction, but only addresses the construction to the extent it materially affects the parties disputes." PO. Resp. 3. Patent Owner contends that "a VPN link does not exist outside of a virtual private network" (*id*. at 4 (emphasis omitted)), a "VPN" requires a network of computers (*id*. at 5), and a VPN link requires "direct communication" (*id*. at 8).

Patent Owner does not provide a clear context as to how the three asserted requirements outlined above materially alter any dispute involved here. Our claim construction does not preclude any of the alleged requirements. In addition, a VPN link is not necessarily the same as a VPN.

For example, when a secure or VPN link extends to a secure network or VPN, one may view the link as part of the VPN or secure network. *See* PO Resp. 6 ("In other words, the VPN communication link and the virtual private network arise contemporaneously and exist between the same devices."). As Petitioner persuasively points out in connection with Figure 33 of the '180 patent, Patent Owner describes the VPN link as a point-to-point link. *See* Pet. Reply 3–4 (citations omitted). That is, Patent Owner asserts that "VPN communication link 3321 traverses the unsecured public network, Internet 3302 to connect computer 3301 with secure server 3320."

[2] Our construction is materially consistent with, but not identical to, the broadest, reasonable construction in *Inter Partes* Reexamination Control No. 95/001,792. *See Cisco Systems, Inc. v. VirnetX, Inc*., Appeal 2014-000491, slip. op. at 4–8 (PTAB Apr. 1, 2014) (Decision on Appeal) (involving the '180 patent).

PO Resp. 6 (describing Fig. 33 of the ’180 patent); *see* Pet. Reply 3–4 (discussing the assertion).

Although Patent Owner maintains that “the VPN communication link is more than a simple connection to a VPN,” Patent Owner’s description of Figure 33, and Figure 33 itself, do not show anything more than a secure link 3321 “travers[ing] the unsecured public network” as Patent Owner otherwise contends. *See* PO Resp. 6 (discussing Ex. 1001, Fig. 33). Figure 33 of the ’180 patent also does not show secure server 3320 behind a firewall or within a virtual private network. *See* PO Resp. 6 (reproducing Fig. 33); Ex. 1001, Fig. 33. Rather, as stated, Figure 33 simply represents a VPN link traversing a public network between two devices (i.e., a link that uses, for example address hopping for security): “[C]ommunications between computers 3301 and 3320 occurs via the VPN [3321], e.g., using a ‘hopping’ regime as discussed above.” Ex. 1001, 52:60–62.

Regarding “direct,” Patent Owner states that it does not impose a “temporal” limitation and does not preclude other intervening nodes, or devices such as routers and which “do not terminate the connection.” Tr. 29:1–30:13. In a related case, the Board found that Patent Owner clarified during an oral hearing involving a challenge to similar claim terms in a grandchild patent to the ’180 patent that Patent Owner did not contend that Provino fails to disclose “direct communication.” *See Apple Inc. v. VirnetX Inc.*, Case IPR2014-00403, slip. op. at 7–8 (PTAB July 29, 2015) (Paper 42) (citing Paper 41(Tr. 86:8–14), Paper 26 (PO Resp. 4) (the “’403IPR”). We made a similar finding in the ’237IPR (Paper 41, 8 n.2, 9–10 (also finding that “the parties don not propose that anonymity is a requirement”). Patent

Owner candidly conceded the same point about "direct" (with respect to Provino) in the oral hearing for this case. Tr. 27:12–24.[3]

Patent Owner also contends that various disclaimers were made regarding the construction of the term "virtual private network communication link" in another reexamination proceeding involving a related patent and a district court proceeding involving six related patents, including the '180 patent. *See* PO Resp. 9–10 (discussing *Inter Partes* Reexamination Control No. 95/001,269, U.S. Patent No. 6,501,135). Patent Owner contends further that the Petitioner agreed with those disclaimers during the respective proceedings. *See*, *e.g.*, PO Resp. 9–10.

Patent Owner made the opposite argument in district court. Ex. 1018, 6 ("VirnetX argues that its statements during reexamination are not a clear disavowal of claim scope."). Patent Owner cannot now rely on any alleged claim disavowals as clear after it characterized them as unclear. *See Tempo Lighting*, 742 F.3d at 978 (The "court . . . 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.")

---

[3] In the '237IPR, the Board addressed *VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir.2014), in which the court addressed the same or similar patent terms. *See* '237IPR, Paper 41, 5–9. In *Cisco*, apparently, neither party appealed the "direct[]" requirement imposed by the district court in the claim construction of a VPN link and secure communication link that *Cisco* adopted. *See Cisco*, 767 F.3d at 1317–19 & n.1. Patent Owner implies that other aspects of the *Cisco* claim construction do "not appear to be relevant to the parties disputes" here. *See* PO Resp. 3 n.1 (referring to "an insecure communication path and techniques other than encryption"—a public path is "insecure" and *Cisco* imposed an anonymity technique as required by a secure communication link (which it deemed to be interchangeable with a VPN), *see Cisco*, 767 F.3d at 1317–19).

Patent Owner's assertion that amending claims in an *inter partes* review proceeding is not a "realistic option" also is not persuasive, because Patent Owner did not move to file an amendment. *See* PO Resp. 8. Under 35 U.S.C. § 316(d)(1), "a patentee may file one motion to amend" and "the opportunity to amend . . . is . . . available." *Cuozzo*, 2015 WL 4097949, at *6.

Accordingly, we maintain our construction of the term "virtual private network" or "virtual private network communication link" for purposes of this decision, albeit with the added (non-material) requirement that the VPN communication link traverses a portion of a public network (which otherwise would be insecure). *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (claim terms need only be construed to the extent necessary to resolve the case).

2. Secure Computer Network Address

We previously construed the term "secure computer network address" to mean "an address that requires authorization for access." Patent Owner does not agree with this construction and argues that one of skill in the art would have broadly but reasonably understood the term "secure computer network address" to require the secure computer network address to be "associated with a computer capable of virtual private network communications." PO Resp. 16. Patent Owner argues that one of ordinary skill in the art would have understood that a "secure computer network address" must be "associated with a computer capable of virtual private network communications," because claim 1 recites "sending an access request message to the secure computer network address using a virtual private network communication link." PO Resp. 16. However, Patent

Owner does not explain sufficiently why an explicitly recited claim limitation must be incorporated into the construction of an associated claim term.

If one of ordinary skill in the art would have understood that all secure computer network addresses must be associated with a computer capable of VPN communications and that any computer network address that is associated with computers that are incapable of VPN communications would be understood not to be a "secure computer network address" (even if authorization for access is required), then any such recited claim limitation would be superfluous.

Patent Owner also argues that "VirnetX's proposed construction has been agreed to by its litigation adversaries and has been adopted by a district court." PO Resp. 15. Even if correct, an adopted agreement between adversaries during litigation in district court need not bind the public at the PTO under a broadest reasonable construction. Patent Owner does not demonstrate persuasively that one of ordinary skill in the art would have construed the term "secure computer network address" to require association with a computer capable of virtual private network communications. Moreover, in the related '403IPR, Patent Owner agreed with the Board's claim construction—the same claim construction involved here. *See* '403IPR, Paper 42, 17 (final written decision, citing Ex. 1090, 21:10–13 (Patent Owner's declarant's testimony); Paper 26, 24 (Patent Owner's response)).

Therefore, we decline to modify our construction of this term.

3. Secure Domain Name

We previously construed the term "secure domain name" to mean "a name that corresponds to a secure computer network address." Patent Owner does not agree with this construction and argues that the term 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)." PO Resp. 17. To support this construction, Patent Owner states that the Specification "'takes pains to explain'" the difference between a "'secure domain name'" and "'a domain name that just happens to be associated with a secure computer.'" PO Resp. 16 (quoting Ex. 1023, 802); *see also* PO Resp. 18–19 (similar arguments, citing Ex. 1001, 52:4–40)).

The Specification discloses an example of "replac[ing] the top-level domain name . . . with a secure top-level domain name." Ex. 1001, 52:19–21. Patent Owner does not demonstrate that the Specification requires a secure domain name to be "non-standard" and fails to explain what the term "non-standard" means. Patent Owner also 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." Ex. 1018, 18 (discussing Patent Owner's arguments during Reexamination Control No. 95/001,270 of the '180 patent) (the "'270 reexamination"). Further, as discussed below, the "resolved" requirement advanced by Patent Owner is embedded in our construction of the claim term "secure domain name service" as set forth below, because the service performs the resolving

function for secure names. Based on the foregoing discussion, we decline to modify our construction of this term.[4]

4. Secure Domain Name Service (SDNS)

Patent Owner proposes that a "secure domain service" (SDNS) should be construed as "[a] lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name." PO Resp. 17. Petitioner proposes that an SDNS should be construed as "[a] service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service [("DNS")] cannot resolve addresses." *See* Pet. 13 (citing Ex. 1011 ¶ 24) (emphasis deleted); PO Resp. 15 (discussing Petitioner's proposed construction). As discussed above, Petitioner's construction largely tracks Patent Owner's proposed construction for the term "secure domain name." The distinction between the two proposals for the term at hand centers on what the function of "recognizes . . . requesting a secure domain name" requires.

To support its construction, Patent Owner argues, among other things, that "during the now-completed *inter partes* reexamination" in the '270 reexamination, "VirnetX . . . disclaimed secure domain services that do not perform this recognition," and, further, the Eastern District of Texas "later relied on VirnetX's statements." PO Resp. 16–17 (citing Ex. 1023, 804 (Response to Office Action, 5 (Apr. 19, 2010), '270 reexamination)); Ex. 1018, 2, 17–19 (District Court Memorandum Opinion and Order)). During the '270 reexamination, Patent Owner contended that an SDNS, as claimed

[4] We need not determine if all secure names are "non-standard," because as discussed below, Provino discloses "non-standard" secure names.

and disclosed, cannot merely "'resolve[] a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name.'" *See* PO Resp. 18 (quoting Ex. 1023, 804).

Patent Owner does not contend explicitly that, or explain how, Petitioner's proposed construction improperly embraces the allegedly disclaimed type of a conventional DNS that "happens" to resolve a domain name query "associated with secure domain name." *See id.* at 17–19. It also is not clear how that allegedly disclaimed feature relates to the "recognizes" function in Patent Owner's proposed claim construction.

Claim 1 recites

> sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name; [and] receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name.

It does not recite "recogniz[ing] that the query message is requesting a secure computer address." "[T]he claims themselves provide substantial guidance as to the meaning of particular claim terms" and "the context in which a term is used in the asserted claim can be highly instructive." *Phillips*, 415 F.3d at 1314. "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Phillips*, 415 F.3d at 1316 (citations omitted).

Based on the context of the claim, the Specification, and the prosecution history, claim 1 does not require "recogniz[ing]" as argued by Patent Owner. As explained in the Background section *supra*, the Specification describes an "SDNS 3313" that "contains a cross-reference

database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name." Ex. 1001, 52:4–8. This disclosure comes closest to aligning with the claim term by explaining how a "secure domain name service" (i.e., an SDNS as set forth in the disclosure) operates. Patent Owner does not point the panel to a disclosure in the Specification that clearly supports the requirement of an SDNS to "recognize that the query message is requesting a secure computer address."

Patent Owner also contends that during the '270 reexamination, Patent Owner proposed various examples of possible "additional functionalities not available with a traditional domain name service." PO Resp. 19. For example, Patent Owner maintains that it argued during the reexamination that a secure domain name service "may allow an entity to register server secure domain names representing different levels of access to the secure website" and "may also support the establishment of a VPN communication link." *See* PO Resp. 19 (citing Ex. 1001, 52:4–40; Ex. 1023, 800, 804). According to Patent Owner, "[t]hus a secure domain service is distinguished from a conventional domain name service." *Id.* (citing Ex. 1023, 804–805).

Contrary to Patent Owner's arguments, even if the prosecution history somehow limits claims that Patent Owner otherwise could have moved to amend under a broadest reasonable construction, Patent Owner's arguments were not "unambiguous," and do not "call for the application of prosecution history disclaimer." *See* PO Resp. 17–18. There was no "express disclaimer," *Bigio*, 381 F.3d at 1325, or "unambiguous disavowal[]," *Grober*, 686 F.3d at 1341.

For example, as Petitioner points out, Patent Owner argued, among other things, as follows during reexamination of the '180 patent:

> *To illustrate, the '180 patent explicitly states 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*. *See*, '180 Patent at col. 51, ll. 18–45 (stating "[b]ecause the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown") . . . .

Ex. 1023, 804 (emphasis added); *see* Pet. Reply 11–12 (discussing prosecution history).

Responding to Patent Owner's various arguments during the reexamination of the '180 patent, the examiner reasoned as follows:

> Further, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, *the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown* ('180 patent, column 51 lines 25–35). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that *can resolve domain names of computers that are used to establish secure connections*. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." *For 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* ('180 patent, column 51 lines 25–35).

’403IPR, Ex. 3001, 3 (Right of Appeal Notice (Dec. 30, 2010), ’180 patent reexamination) (emphases added, examiner’s emphasis omitted).[5]

This exchange between the Patent Owner and the examiner reveals that the central reason for confirmation by the examiner in the ’180 patent reexamination was Patent Owner’s argument that the ’180 patent makes clear that a conventional DNS *cannot resolve addresses for a secure domain name*, whereas the disclosed SDNS can. *Id.*

Petitioner contends that the declarants for Patent Owner and Petitioner essentially agree to this key distinction. *See* Pet. Reply 7–9 (citing Ex. 1089, 16:21–17:18, 19:19–21; Ex. 1088, 16:9–7:17; 21:14–22:1, 23:16–26:15; Ex. 1011 ¶ 15.). Quoting the ’180 patent, Dr. Roch Guerin, Petitioner’s declarant, testifies that it “indicates that ‘SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses.’ Ex. 1001, 52:4–5. In other words, *the SDNS 3313 differs from a standard name service in that it is configured to resolve secure domain names*.” Ex. 1011 ¶ 15 (emphasis added). After summarizing other pertinent disclosures in the ’180 patent Specification (*see* Ex. 1011 ¶¶ 11–23), Dr. Guerin testifies that “a broadest reasonable interpretation of ‘secure domain name service’ would be broad enough to cover ‘a service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses.’” Ex. 1011 ¶ 24.

Dr. Fabian Monrose, Patent Owner’s declarant, testified during cross-examination that a “secure domain name service is referred to as a lookup

[5] Page number “3” in Ex. 3001 refers to the original page number supplied by the examiner in the Right of Appeal Notice.

service that recognizes that a query message is requesting a secure computer address and returns a secure computer address for the requested secure domain name." Ex. 1088, 21:18–22. Arguing that Provino does not disclose an SDNS, Patent Owner relies on Dr. Monrose's declaration testimony that the disclosed SDNS does more than provide a mere look-up function. *See* PO Resp. 30–32 (citing Ex. 2024 ¶¶ 35–39); *see also* Ex. 1088, 17:22–18:4 (Dr. Monrose's deposition testimony: "For example, the ability to initiate a virtual private network communication, the ability to have multiple levels of access control, the ability to make decisions based on the -- on the originator, et cetera."). Similar to this declaration and deposition testimony, Patent Owner lists different "additional functionalities not available with a traditional domain name service. For instance, a secure domain service may allow an entity to register server secure domain names representing different levels of access to the secure website." *See* PO Resp. 19 (citing Ex. 1023, 804; Ex. 1001, 52:4–40).

Even if these types of "example[s]" describe possible functions of a disclosed SDNS, they do not arise to an unequivocal disclaimer or show that the "recognizes" function must be incorporated into the claimed SDNS. Dr. Monrose and Patent Owner do not offer a clear interpretation of what the "recognizes" function entails and do not point to where that term appears in the '180 patent Specification. Describing "some examples" of what some of the disclosed "SDNS[] . . . embodiments . . . can perform" fails to link those examples with the proffered "recognizes" function. *See* Ex. 1088, 21:18–22:5. In other words, Dr. Guerin's testimony and Petitioner's claim construction tracks more closely to direct support in the '180 patent Specification.

Further alleging a Specification disclaimer, Patent Owner quotes the '180 patent as noting that '"[t]he conventional scheme suffers from certain drawbacks,'" and points to "'certain aspects of the invention'" as setting up a VPN. PO Resp. 33 (quoting Ex. 1001, 39:63–40:24 (emphasis by Patent Owner), citing Ex. 2041 ¶ 35). In that conventional scheme, the '180 patent discloses that "[o]ne conventional *scheme* . . . provides the DNS server with public keys of the machines that the DNS server has addresses for." Ex. 1001, 40:6–8 (emphasis added). The '180 patent describes "drawbacks" pertaining to that "conventional *scheme*" (i.e., not the DNS or an SDNS itself): "For example, any user can perform a DNS request. . . . [and] DNS requests resolve to the same value for all users." Ex. 1001, 40:15–17 (emphasis added).

Although it is not clear, this disparaged "scheme" may be the basis upon which Patent Owner relies for its disclaimer argument that an SDNS cannot merely resolve a domain name query that "just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization" with a secure domain name. *See* PO Resp. 16 (citing Ex. 1023, 802, 803, but not linking directly the disclosed conventional public key scheme to the prosecution argument); *see also* PO Resp. 31–33 (discussing disclaimer as allegedly distinguishing over Provino).

Nevertheless, Patent Owner fails to explain how Petitioner's construction embraces this disparaged public key scheme that may happen to return a public key. As noted above, Petitioner proposes that an SDNS "can resolve secure computer network addresses for a *secure domain name*." Pet. 13 (emphasis added, emphasis by Petitioner deleted). On its face, a "secure

domain name" does not "happen" to be "associated with a secure name"; rather, a secure domain name *is* a secure name.

Moreover, the '180 patent describes overcoming the problems associated with the public key "scheme" by doing much more than adding Patent Owner's proposed "recognizing" functionality to the SDNS as construed by Petitioner:

> According to *certain aspects* of the invention, a *specialized* DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communications are defined), *the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user*. The VPN is preferably implemented using the IP address "hopping features."

Ex. 1001, 40:18–35 (emphases added). The claims do not recite a "specialized DNS," but even if the claimed SDNS somehow relates to this disclosed "specialized DNS," Patent Owner does not urge that its proposed SDNS must return a false IP address, automatically set up a VPN, or use hopping features—all of which the Specification discloses as solving problems associated with the allegedly disparaged conventional DNS/public key scheme.

Patent Owner also does not explain how its proposed "recognizes" functionality would overcome the conventional scheme's problem of allowing "any user [to] perform a DNS request," or prevent its proposed SDNS from "resolv[ing] the same value for all users." *See id*. at 40:16–17. On this record, a "secure network address is an address that requires authorization for access." As noted above, in the '403IPR, Patent Owner agreed with this claim construction. *See* '403IPR, Paper 42, 17 (citing Ex. 1090, 21:10–13 (Patent Owner's declarant's testimony); Paper 26, 24 (Patent

Owner's response)); *supra* Section I.E.2. Assuming that "any user" has knowledge of a specific secure domain name, a secure network address that requires authorization naturally prevents "any user" from obtaining it via a resolved secure domain name, thereby overcoming the prior art problems in the DNS conventional scheme, and suggesting that any "recognizes" functionality as a proposed SDNS requirement would be superfluous or not required.

Overcoming that prior art scheme's problems with a list of disclosed features that are not required under Patent Owner's claim construction fails to support that construction. Criticizing a prior art *scheme* in the disclosure or in arguments does not criticize an SDNS itself. As a specific example, urging construction of a client computer as a user's computer, Patent Owner refers to a "conventional" "user's" computer as "another embodiment," even though the '180 patent Specification disparages the "conventional architecture" that employs such a user's computer (because it is not secure enough). *See* Ex. 1001, 39:53–40:5; PO Resp. 21. As Petitioner notes with regard to the allegedly disparaged public key/DNS scheme, "'[m]ere criticism of a particular embodiment encompassed in the plain meaning of a claim term is not sufficient to rise to the level of clear disavowal.'" Pet. Reply 8 (quoting *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1366 (Fed. Cir. 2012)).

Further, as Petitioner persuasively argues, "the '180 patent itself shows systems that use standard domain name services as part of the purported invention and Patent Owner's expert admits as much." Pet. Reply 8 (citing Ex. 1001, Fig. 26, 40:46–41:8; Ex. 1089, 15:22–16:12). At the cited deposition passage, Dr. Monrose acknowledges that the '180 patent

Specification states that "[a] modified DNS server 2602 includes a conventional DNS server function 2609." Ex. 1001, 40:41–42; Ex. 1089, 15:22–16:12 (discussing Ex. 1001, Fig. 26 and the related passages). Dr. Monrose also agrees that modified DNS server 2602 corresponds to the claimed SDNS. Ex. 1089, 17:19–18:2. The '180 patent Specification adds that the modified DNS also includes a "DNS proxy 2610," but that proxy "determines whether access to a secure site has been requested . . . for example, by a domain name extension, *or by reference to an internal table of such sites*." Ex. 1001, 40:47–51 (emphasis added).

In other words, the SDNS and DNS each include simple look-up functionality—the former includes secure names for secure devices in an internal table and the latter does not. Patent Owner cannot attempt to disavow that disclosed functionality by attempting to add unclaimed features from the Specification. In any event, Petitioner's construction distinguishes over a conventional (i.e., a non-secure) DNS that does not provide a look-up for secure devices based on a secure domain name.

During the oral hearing in the related '403IPR, when questioned about the specific added functionality the claims may require by disclaimer or otherwise, Patent Owner indicated that the claims do not require a specific functionality:

> Because in some instances it could be example A and in some instances it could be example B. But as long as it is recognizing that a query message is requesting a secure . . . computer address . . . it can't be just a conventional DNS operation. It has to be more than that.

'403IPR, Paper 47, 67:24–68:4.

In light of the record, the clearest thread running through the arguments, prosecution history, evidence, the '180 patent Specification, and

the claim language, is that "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* ('180 patent, column 51 lines 25–35)." '403IPR, Ex. 3001, 3 (emphasis added). Simply put, a conventional DNS does not resolve a *secure* address for a *secure* domain name, hence the different name, *secure* domain server, and nomenclature, SDNS. *Cf. In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1150 (Fed. Cir. 2004) (disavowal must "repeatedly, consistently, and exclusively" show the same feature).

Patent Owner made the opposite argument to the District Court that it is making here, and argued that the "non-standard" distinction (which somehow underlies the "recognizing" requirement according to Patent Owner's arguments here) "is not supported by the specification or the prosecution history." Ex. 1018, 18 (discussing Patent Owner's '270 reexamination prosecution history arguments). In other words, *despite* Patent Owner's arguments to the contrary in the District Court, the District Court found against Patent Owner, and reasoned that Patent Owner had "explained 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.'" *Id.* (quoting argument by Patent Owner) (emphasis omitted). Therefore, the District Court stated that "[a]ccordingly, the non-standard characterization proposed by *Defendants* should be retained." *Id.* (emphasis added).

The District Court then construed a "secure domain name service" as a "non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network

address for a requested secure domain name." *Id.* at 19. Nevertheless, in arguments and reasons presented on this record and in the District Court, Patent Owner unequivocally "explained 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.'" *See id.* at 18 (quoting argument by Patent Owner) (emphasis omitted).

Accordingly, with a record that is distinct from that in the reexamination and the District Court, and employing a broader claim construction standard than the District Court, we adopt Petitioner's proposed construction, which tracks Patent Owner's repeated argument and the '180 patent Specification that all show that an SDNS is "[a] service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service [("DNS")] cannot resolve addresses."

Patent Owner concludes that it is bound by its disclaimers and "precluded from arguing for a broader construction." PO Resp. 17. Patent Owner may be bound only by clear unequivocal disclaimers in district courts or with respect to unexpired patents that return to the USPTO. Unlike in a district court, Patent Owner here had the opportunity to propose claim amendments that include the "recognizes" functionality urged, but chose not to do so. In addition, Patent Owner did not amend claims to address and clarify an SDNS during the original prosecution history for the '180 patent. These factors weigh against finding prosecution history disclaimer, especially where any disclaimer is equivocal at best. *See Tempo Lighting*, 742 F.3d at 978 ("This 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. However, in this instance, the PTO itself requested Tivoli rewrite the 'non-photoluminescent' limitation in positive terms. Tivoli complied, and then supplied clarification about the meaning of the 'inert to light' limitation.").[6] In any event, Petitioner's proposed claim construction reasonably accounts for any clear disclaimer.

Based on the foregoing discussion and the record, we adopt Petitioner's proposed construction and do not adopt Patent Owner's proposed construction of the term "secure domain service."

5. Client Computer

Patent Owner contends that this term is "material to several claims and should be construed." PO Resp. 20. Patent Owner also contends that "the broadest reasonable interpretation of 'client computer' is a 'user's computer.'" *Id*. Patent Owner does not contend that Provino fails to disclose a user's computer, or a client computer as set forth in any of the claims.

Therefore, this term does not appear to be material in this proceeding. In any event, to the extent it is material, the '180 patent Specification employs the term "user's computer" in a "conventional scheme . . . shown in FIG 25. A user's computer 2501 includes a client application 2504 (for example a web browser) . . . ." Ex. 1001, 39:53–55. Although Patent Owner refers to this "conventional" computer as "another embodiment," the

[6] In *Tempo Lighting*, the original prosecution creating the disclaimer that the PTO was "under no obligation to accept" was closed, and the Board employed that original record as part of the intrinsic record to shed light on the meaning of the claim during an appeal of a subsequent reexamination. 742 F.3d at 978–79.

'180 patent Specification disparages the "conventional architecture" that employs a user's computer, because it is not secure enough. *See id*. at 39:53–40:5; PO Resp. 21. In general, the '180 patent Specification states that "[t]he present invention" involves a "client computer" with a "client application" that "communicates with a server." *See* Ex. 1001, 7:43–50. This description of "[t]he present invention" does not mention, let alone require, a "user's computer."

Therefore, contrary to Patent Owner's arguments, the '180 patent Specification does not repeatedly treat a "client computer" and a "user's computer" as the same. The broadest reasonable construction of a client computer is a computer associated with a client.

6. Access Request Message

As Patent Owner explains, the construction of this term "do[es] not appear to be relevant to the parties' disputes." PO Resp. 23.

II. ANALYSIS

A. Anticipation, Provino

For at least the reasons discussed below, we find that Petitioner has demonstrated that Provino anticipates claims 1, 10, 12–15, 17, 26, 28–31, and 33 under 35 U.S.C. § 102.

1) Receiving a Secure Domain Name

Claim 1 recites "receiving a secure domain name." (Ex. 1001, claim 1.) Patent Owner notes that "[i]ndependent claims 17 and 33 recite similar features." PO Resp. 26.

Patent Owner argues that Provino does not disclose the claim feature because nameserver 32 does not "verif[y] the domain name as secure, as alleged by the Decision." *Id*. at 27 (citing Inst. Dec. 14). Petitioner notes

that under the claim construction of a "secure domain name" as "a name that corresponds to a secure computer network address," "Patent Owner . . . concedes Provino discloses this limitation." Pet. Reply 6–7 (citing Ex. 1003, 13:31–40, 10:45–67; Resp. 26; Ex. 2024 ¶ 28; Ex. 1011 ¶¶ 29–33; Inst. Dec. 8). Petitioner's argument and showing is persuasive. The claim element does not require any verification that the name is secure.[7]

Patent Owner also argues that Provino does not teach "receiving a secure domain name" because Provino uses "standard" domain names. PO Resp. 29. Patent Owner points to its Specification that allegedly discusses "an exemplary 'standard' domain name ending in '.com' and an exemplary 'non-standard' domain name ending in 'scom.'" PO Resp. 28 (citing Ex. 1001, 51:16–17; Ex. 2024 ¶ 31).

These exemplary embodiments do not alter the broadest reasonable claim construction of a "secure domain name." *See supra* Section I.E.3., I.E.4. (Claim Construction). As also noted above (*id*.), Patent Owner made the opposite argument to a district court, and argued that a "non-standard" distinction "is not supported by the specification or the prosecution history." Ex. 1018, 18.

Even if the disputed term requires a non-standard domain name, as Petitioner points out, Provino's "'invention can be used in connection with

[7] In our Institution Decision, we stated that "*Petitioner also explains* that nameserver 32 verifies the domain name as secure and associates it with a secure network address, as provided to device 12(m) for future secure communications." Inst. Dec. 14 (emphasis added). Even if "verifies" (or "recognizes") is a claim requirement (each is not), Provino's system returns secure addresses to a firewall, as explained further below, thereby verifying or recognizing a name as secure. *See* Ex. 1001, 11:21–23.

any network which provides for *any form of a secondary or informal network address arrangement*.'" Pet. Reply 7 (quoting Ex. 1003, 16:12–17; citing Ex. 1011 ¶¶ 34–35) (emphasis by Petitioner). Dr. Guerin's testimony cites to Provino and shows persuasively that Provino discloses a "non-standard domain name that corresponds to a secure computer network address (i.e., integer Internet address of the server 31(s)) and cannot be resolved by a conventional domain name service (DNS)." Ex. 1011 ¶ 34 (citing Ex. 1003, 16–17).

Patent Owner responds to Provino's disclosure by characterizing it as "take[n] out of context . . . [and] part of a brief discussion at the end of the patent mentioning that *Provino*'s system can be used in other types of networks although *Provino* only describes it in the context of the Internet. PO Resp. 28 (citing Ex. 1003, 16:8–16; Ex. 2024 ¶ 32). This argument fails to rebut Petitioner's showing (i.e., even if a "secure domain name" requires a non-standard name). Brief discussions constitute disclosures; Patent Owner fails to explain how Provino's disclosure is out of context; and Patent Owner does not explain how "the context of the Internet" or "use[] in other types of networks" has a material bearing to a claim term at issue. *See id*.

Dr. Monrose's cited testimony on the point parrots Patent Owner's arguments and is not persuasive. *See* Ex. 2024 ¶ 31. Dr. Monrose notes that Provino provides human readable Internet addresses to "'relieve a user of the necessity of remembering and entering specific integer Internet addresses.'" *Id*. ¶ 31 (quoting Ex. 1003, 1:49–52). Despite this disclosure and the above-discussed disclosure of "any form of a secondary or informal network address arrangement" (Ex. 1003, 16:12–17), which show that Provino's human readable names include non-standard domain names, Dr. Monrose

reasons that these "human readable Internet addresses" are not "non-standard" because "*Provino is not concerned* with 'standard' versus 'non-standard' domain names in its system." Ex. 2024 ¶ 31 (emphasis added). This reasoning effectively reduces to an *ipsissimis verbis* test by requiring Provino to discuss exact claim terms. For anticipation, "the reference need not satisfy an *ipsissimis verbis* test." *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009).

Based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that Provino discloses receiving a secure domain name as recited in claims 1, 17, and 33.

2) Sending a Query Message to a Secure Domain Name Service, the Query Message Requesting From the Secure Domain Name Service a Secure Computer Network Address Corresponding to the Secure Domain Name

Patent Owner argues that Provino does not disclose the above recited claim 1 phrase, because "*Provino's* nameserver 32 is not the claimed 'secure domain name service' in light of the '180 patent's disclosure, prosecution history disclaimer, and Petitioner's own construction." PO Resp. 29. This argument is not persuasive because the claimed SDNS reads on Provino's nameserver 32 as explained in the next section.

3) Secure Domain Name Service

Claims 1, 17, and 33 recite a "secure domain name service" (SDNS). Patent Owner argues that Provino's VPN Name Server 32 is not an SDNS because "nameserver 32 behaves just like nameserver 17, which Petitioner concedes is a conventional DNS." PO Resp. 37 (citing Pet. 19; Ex. 1011, 18; Dec. 9). Patent Owner's argument is not persuasive and largely turns on Patent Owner's overly narrow claim construction of SDNS, which we do not adopt. *See supra* Section I.E.4 (Claim Construction).

Patent Owner does not dispute, as Petitioner contends, that Provino's nameserver 32 resolves secure domain names into secure network addresses. *See* PO Resp. 37–38; Pet. Reply 8–10. Rather, Patent Owner contends that "the mere fact that a DNS can resolve domain names that another DNS cannot resolve does not make it a secure domain name service . . . and the Board has rejected Apple's argument to the contrary." *Id*. (citing Inst. Dec. 9; Ex. 2024 ¶ 39).

The latter argument that the Board "rejected Apple's argument" mischaracterizes the Institution Decision and the issue involved here. We determined that "for purposes of this Decision, a 'secure domain name service' is a service that provides a secure computer network address for a requested secure domain name." Inst. Dec. 9. If anything, this prior claim construction is a slightly broader construction than Petitioner's proposed construction that we adopt for this Final Written Decision.

Further, Provino's VPN nameserver 32 resides behind a firewall, which controls access to secure devices 31(s), indicating, according to *Cisco*, a secure domain name service—i.e., providing a secure service for secure devices.[8] *See* Ex. 1003, Fig. 1, 9:6–17. Patent Owner's argument that

[8] *See Cisco*, 767 F.3d at 1322 ("VirnetX provided substantial evidence for the jury to conclude that paths beyond the VPN server may be rendered secure and anonymous by means of 'physical security' present in the private corporate networks connected to by VPN On Demand."). Underlying that finding, the *Cisco* court noted that "VirnetX's expert testified that one of ordinary skill would understand that the path . . . within the private network[] would be secure and anonymous owing to the protection provided by the private network." *Id*. at 1321.

nameservers 17 and 32 perform similar functions simply demonstrates that they are both nameservers. *See* PO Resp. 37–38.

In addition, Provino's SDNS 32 "is generally similar to . . . nameserver [17], *except* that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m)." Ex. 1003, 11:20–25 (emphasis added). In other words, even under Patent Owner's narrow claim construction that requires an SDNS to perform an additional function (i.e., in addition to resolving a secure domain name (*see* PO Resp. 16–18)), unlike conventional nameserver 17, secure nameserver 32 directs a message packet to firewall 30, and thereby performs that additional function (i.e., implicitly "recognizing" that the request is for a secure address).

Discussing Provino's nameserver 32 and relying on Dr. Monrose, Patent Owner argues that "when nameserver 32 receives a human-readable address, it simply checks 'whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet,' and, if so, 'generate[s] a response message packet including the integer Internet address for transmission to the firewall.'" PO Resp. 37–38 (quoting Ex. 1003, 14:39–46; citing Ex. 2024 ¶ 40).

Patent Owner contends that this and other similar operations show that nameserver 17 and secure nameserver 32 behave the same, rendering secure name server 32 a conventional DNS that a proper claim construction does not embrace. *See id*. Setting aside the additional functionality that Provino's name server 32 provides as discussed above (sending packets to a

firewall), Patent Owner's arguments rest unpersuasively on Patent Owner's overly narrow and non-adopted claim construction.

Patent Owner's response does not dispute that Provino's secure nameserver 32 operates differently from nameserver 17 in a critical fashion, as Petitioner argues: "Provino itself distinguishes nameserver 32 from public nameserver 17, and Patent Owner's expert agrees that nameserver 17 ***cannot*** resolve queries for ***secure*** network addresses because [they do] not have network addresses for ***secure*** devices behind firewall 30 of VPN 15 (as nameserver 32 does)." Pet. Reply 10 (comparing the disclosed invention to Provino's similar secure nameserver 32, citing Ex 1003, 10:45–55, 11:11–14, Ex. 1011 ¶¶ 14, 30, 34; Ex. 1001, 51:29–35; Ex. 2019, 61:18–63:2).

Despite Patent Owner's arguments (*see* PO Resp. 30–38), as discussed *supra* in the Claim Construction section (Section I.E.4.), Patent Owner has not disparaged or disavowed, unequivocally, a "secure domain name service," as set forth in the claims, which resolves a secure domain name. *See* Pet. Reply 8–9. Patent Owner contends that it also argued during reexamination of a related patent, U.S. Patent No. 8,051,181, that *Provino*'s "nameserver 32 is a conventional DNS server that does not resolve secure names." PO Resp. 35 (citing Ex. 2020, 13; Ex. 2021, 50; Ex. 2022, 30 (characterizing prosecution history arguments respectively in a rebuttal brief, appeal brief, and patent owner's response in Reexamination Control No. 95/001,949). Patent Owner does not make this argument explicitly here, but in any case, close inspection reveals that Patent Owner's prosecution argument is circular: "Without a secure domain name server, *Provino* cannot disclose secure names." Ex. 2022, 30.

Further, Patent Owner correctly states in the appeal brief in the 95/001,949 reexamination that "the examiner . . . refuse[s] to give effect to the disclaimer." Ex. 2021, 41. In other words, no disclaimer exists here based on Patent Owner's circular argument made during the 95/001,949 reexamination, and the examiner maintained the rejections based *inter alia*, on Provino, with similar findings, which Patent Owner appealed.[9]

In that same appeal brief, Patent Owner describes Provino's nameserver 17 and nameserver 32 as differing in that the former "resolves names for devices located outside the firewall" and the latter "operates in a similar manner except it resolves addresses for servers 31(S) behind firewall 30." Ex. 2021, 41. Patent Owner argues similarly in that appeal brief that the firewall does not show that nameserver 32 resolves secure names. *Id*. As noted above, this contradicts findings and rationale in *Cisco* (quoted and cited *supra* notes 3 and 8)—for example, that devices are "secure and anonymous by means of 'physical security' present in . . . private corporate networks," 767 F.3d at 1322.

As Dr. Guerin testifies, Provino's secure nameserver 32 provides an Internet address for secure server 31(s) (behind the firewall) that nameserver 17 cannot provide. *See* Ex. 1011 ¶¶ 35–36; Ex. 1003, 11:5–25, 15:21–30, Fig. 1. As Petitioner contends, there is no reasonable dispute, if any, on this record about that "key difference," which the claim construction of "secure domain name service" captures. *See* Pet. Reply 9 (citing Ex. 1089, 16:21–17:18, 19:19–21, 49:9–50:12; Ex. 1088, 16:9–17:17, 21:14–22:1, 23:16–

[9] *See* the 95/001,949 reexamination, Appeal Docketing Notice (Mar. 21, 2015)(assigning Appeal No. 2015-004512); Right of Appeal Notice (Aug. 16, 2013).

26:15, 38:22–40:18; Ex. 1011 ¶ 15); PO Resp. 25 (describing Provino's system, stating "[w]hen nameserver 17 receives a request for the address of server 31(s) on virtual private network 15, however, it may return the address of firewall 30 on virtual private network 15 because it does not have the address of server 31(s)").

As Provino explains, "[s]ince nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m)"—i.e., the integer Internet address associated with secure server 31(s)—"it will send a response . . . so indicating." Ex. 1003, 11:10–13. Turning to nameserver 32, Dr. Monrose testifies during his deposition, and Patent Owner agrees, that Provino's nameserver 32 will attempt to resolve the address of server 31(s)—if it "knows the address of server 31 and that can be provided to device 12M." Ex. 1089, 50:11–12; *see also* PO Resp. 37–38 (quoting Ex. 1003, 14:39–46; citing Ex. 2024 ¶ 40) (describing operation of nameserver 32).

Based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that Provino discloses a "secure domain name service" as recited in claims 1, 17, and 33.

4) Access Request Message

Patent Owner argues that Provino does not disclose "sending an access request message from the first network device to the secure network address using a virtual private network communication link," as claims 1, 17, and 33 recite, because

> *Provino* does not disclose what the message packets sent from device 12(m) to server 31(s) do, let alone whether the message packets sent to server 31(s) include a signal that "signifies that the [device 12(m)] seeks communication, information, or

> services, with or from [server 31(s)]," as required by the Decision's construction of "access request message."

PO Resp. 39 (discussing Inst. Dec. 6).[10]

Patent Owner argues that the Institution Decision relies on "inherency," and implies that Provino does not disclose that the message packets "necessarily" request access to servers 31(s). *Id.* Petitioner responds by noting that it relies on what Provino describes about known servers, implicitly or otherwise, to ordinarily skilled artisans. *See* Pet. Reply 12–13; *In re Preda*, 401 F.2d 825, 826 (CCPA 1968) ("[I]t is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom.").

In general, after obtaining the secure network address for server 31(s) and decrypting it, Provino's network device 12(m) uses it to communicate with server 31(s) by sending message packets thereto. *See* Ex. 1003, 15:27–30. Petitioner points out that Patent Owner's declarant agreed during his deposition that "request[ing] access to whatever information is stored on server 31S . . . could be one reason to connect to 31S." Pet. Reply. 12 (citing Ex. 1088, 42:12–43:10) (emphasis omitted).

Petitioner also relies on Dr. Guerin, who testifies as follows:

> Once the device 12(m) obtains the integer Internet address of server 31(s) from nameserver 32 during the second phase of establishing communications with server 31(s), the

[10] Patent Owner raises another independent timing-based argument concerning the access request and tunnel set-up that we need not reach here, because this Final Written Decision does not rely on the independent findings that are the focus of the arguments. *See* PO Resp. 40–45; Inst. Dec. 42.

> device 12(m) may send access requests to server 31(s) using the secure tunnel established with the firewall 30 in the first phase of the communication process. *See* Ex. 1003, 15:21–30. In particular, Provino describes that the server 31(s) may be a "storage server" that provides information that is requested by a client. *See* Ex. 1003, 6:19–50. As a consequence, the requests sent to server 31(s) by device 12(m) may be requests for information stored at the server 31(s). By describing that device 12(m) generates a message packet for transmission to server 31(s) and receives information transferred from server 31(s), Provino describes that device 12(m) leverages the resolved secure computer network address (i.e., integer Internet address) to send access request messages to server 31(s) that contain requests for access to information stored on server 31(s).

Ex. 1011 ¶ 39; *see* Pet. 12–13 (discussing *id.*, citing Ex. 1089, 41:12–42:31; Ex. 1003, 6:19–28, 6:64–7:7).

Provino corroborates Dr. Guerin. Generally, Provino's ultimate goal is to "provide[] a system for easing communications between devices" in a secure tunnel through a firewall that defines or corresponds to a VPN. Ex. 1003, 15:59–60. The communicating devices include servers, personal computers, workstations, and other similar devices that operate in a "client-server" relationship, where requesting client device 12(m), for example, can "initiate service," and server 31(s), or a similar device, can "perform processing operations at the request of the client," or "provide information to the client." *Id.* at 6:31–50.

As Dr. Guerin describes, Provino describes one embodiment wherein server 31(s) is a storage server, which provides information requested by first network device 12(m) in a client-server relationship. *See* Ex. 1003, 6:19–50; Ex. 1011 ¶¶ 39–40. "If the server is to provide information to the device, it (that is, the server) may generally be referred to as a storage

server." Ex. 1003, 6:43–45. The devices "communicate by transferring message[s] . . . over the Internet." *Id.* at 6:30–31. The message itself identifies "the intended recipient of the message packet" which may be "another device, such as server 31(s)." *Id.* at 10:31–33.

> Provino also describes that after setting up the secure tunnel,
>
> the integer Internet address for the server 31(s) can be cached in an *access* control list ("ACL") in the IP parameter store 25 [of access requesting device 12(m)], along with the association of the human-readable Internet address thereto, an indication that the server 31(s) . . . is *to be accessed* through the firewall 30 of the virtual private network 15.

Ex. 1003, 11:35–41 (emphases added). In other words, Provino describes that "the server 31(*s*) is *to be accessed*," using a "message packet" or "message packets." *See id*. at 11:13–45 (emphasis added).

Patent Owner makes the same or similar arguments with respect to claims 12 and 28, which depend respectively from independent claims 1 and 17. PO Resp. 45–46. Claims 12 and 28 recite "wherein the access request message contains a request for information stored at the secure computer network address." In addition to the above-discussed arguments, Patent Owner notes that "the packets might serve a different purpose entirely, such as to request that *information be stored* on server 31(s). . . . or might send the content of its internal storage device to server 31(s) for backup storage." *Id*. at 46 (emphasis omitted and added). These arguments support (rather than rebut) the above-discussed findings that show that skilled artisans would have recognized from Provino's disclosure that in addition to whatever else Provino's typical storage server 31(s) might do according to Patent Owner (including storing information), it also processes packets containing requests for such information, thereby anticipating claims 1, 12,

17, 28, and 33. Ordinarily skilled artisans armed with common sense would have recognized that servers store information to provide subsequent access thereto.

Based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that Provino discloses a "request message packet" and the other limitations recited in claims 1, 12, 17, 28, and 33.

5) Claims 10 and 26

In addition to its arguments discussed above in connection with independent claims 1, 17, and 33, Patent Owner contends for another reason that Provino does not anticipate claims 10 and 26, which depend respectively from independent claims 1 and 17. PO Resp. 43–44. Claims 10 and 26 recite "wherein the virtual private network includes the Internet." According to Patent Owner, Provino discloses using the Internet; however, as to "the independent claims, [Petitioner] relied on a separate, undescribed embodiment where *Provino*'s system is implemented on 'any network' other than the Internet to support its incorrect view that *Provino*'s human-readable addresses are 'non-standard' names." PO Resp. 43. According further to Patent Owner, Petitioner "cannot . . . rely on a non-Internet embodiment of *Provino* for the independent claims while simultaneously relying on the Internet embodiment of *Provino* for the dependent claims." *Id*. at 43–44.

First, Patent Owner's argument incorrectly assumes that the independent claims require a non-standard name (alleged to be in a "non-Internet embodiment"). Second, even if they do under an overly narrow and non-adopted construction urged by Patent Owner, Figure 1 of Provino, the sole figure, schematically discloses a VPN in the form of a secure tunnel

employed over the Internet from device 12(m) to secure server 31(s) behind firewall 30. *See* Ex. 1001, Fig. 1; Ex. 1003, 12:1–16.[11] Provino does not limit its teachings about non-standard domain names to "'any network' other than the Internet." *See* PO Resp. 43. Rather, we find that Provino describes "a network" as "the Internet" and that "any network" includes "the Internet," as the following passage shows:

> [A]though the *invention* has been described in connection with the *Internet*, it will be appreciated that the *invention* can be used in connection with *any network*. Further, *although the invention* has been described in connection with *a network* which provides for *human-readable network addresses*, it will be appreciated that the *invention* can be used in connection with *any network which provides for any form of secondary or informal network address arrangements*.

Ex. 1003, 16:8–17 (emphases added).

This passage shows that Provino includes the Internet as "a network." Patent Owner's argument reduces to the untenable assertion that Provino's disclosure somehow conveys to ordinary artisans that "any network" excludes "a network" and the Internet, and that only "any network" (which somehow excludes the Internet) carries "any form of secondary or informal network address arrangements."

Provino describes generally establishing a secure tunnel "in connection with the Internet" and resolving "human-readable Internet addresses." Ex. 1003, 16:1–16, *see also* Fig. 1 (showing Internet 14 and VPN 15); Pet. 29–30 (addressing claim 10). Based on Provino's above-

[11] The tunnel extends over Internet 14 to VPN 15 to create an extended "virtual" private network—i.e., a VPN as required by claims 10 and 28. *Compare* Ex. 1003, Fig. 1, *with* Ex. 1001, Fig. 33 and PO Resp. 6 (discussing Fig. 33); *see supra* Claim Construction (section I.E.1).

discussed descriptions pertaining to the issue and the testimony of Dr. Guerin (Ex. 1011 ¶ 34), we find that Provino discloses using non-standard or standard domain names on any network including the Internet. Stated differently, we find that Provino does not segregate the use of non-standard domain names to non-Internet networks. We also find that Provino supports the testimony of Dr. Guerin on this point: "[T]he VPN 15 [depicted in Figure 1, which also depicts the Internet 14] described by Provino is configured to support nonstandard human readable domain names." Ex. 1011 ¶ 34.

5) Claims 13–15 and 29–31

Patent Owner relies on arguments presented for patentability of independent claims 1, 17, and 33 to rebut Petitioner's showing that Provino anticipates dependent claims 13–15 and 29–31. PO Resp. 46.

Based on further review of the record, including the Petition and its supporting evidence, and for the reasons discussed *supra* in connection with claims 1, 17, and 33, we find that Petitioner shows by a preponderance of evidence that Provino anticipates dependent claims 13–15 and 29–31. *See* Pet. 15–35.

B. Obviousness, Claims 4, 6, 20, 22, 35, and 37

Claims 4, 20, and 35 respectively depend from independent claims 1, 17, and 33, and recite "wherein the response message contains provisioning information for the virtual private network." The "response message" refers to the message received from the secure domain name service in the independent claims. Claims 6, 30, and 37 respectively depend from claims 4, 20, and 35. Patent Owner does not present separate arguments for claims 6, 30, and 37, and focuses on claims 4, 20, and 35. *See* PO Resp. 48–51.

In addition to the above-discussed arguments, Patent Owner argues that the combination of Provino and Guillen cannot render obvious claims 4, 20, and 35 without another reference cited in the Petition and relied upon by Dr. Guerin in his declaration testimony— a prior art reference to Kosiur. PO Resp. 47–48. According to Patent Owner, "without this link, which one of ordinary skill in the art would not have made for the reasons discussed in the next section, the ground is conclusory because it lacks the required 'articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" PO Resp. 48 (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006))).[12]

Patent Owner's argument on this point seems to imply that Kosiur, cited by Dr. Guerin, otherwise renders the combination obvious. *See* Ex. 1041 ¶¶ 42. Patent Owner did not move to exclude Dr. Guerin's testimony that cites to Kosiur, which is of record. Ex. 1006. On the other hand, Patent Owner correctly points out that the Institution Decision does not consider Kosiur to be included in the ground of obviousness. PO Resp. 47; Inst. Dec. 19 n.1. On this record, we exercise our discretion and decline to consider Kosiur.

Without Kosiur, Patent Owner contends that a skilled artisan would not have combined Guillen's system with Provino's system because Guillen discloses providing QoS information "before establishing the Virtual

[12] "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Kahn*, 441 F.3d at 988.

Circuit"; therefore, "*Guillen*'s QoS information would be moot after [Provino's] tunnel is established." PO Resp. 50. Patent Owner also contends that "providing [Guillen's] QoS information in a directory service [such as Provino's nameserver 32]. . . is so 'the user will have an indication of what is feasible' before establishing the Virtual Circuit" that Guillen discusses. PO Resp. 50 (citing Ex. 1005, 82; citing Ex. 2024 ¶ 52).

> Petitioner responds to Patent Owner's argument as follows:
>
> [I]n Provino, ***before*** this path between device 12(M) and server 31(s) can exist, nameserver 32 must provide server 31(s)'s secure address. . . . If, in the same response message, a modified nameserver 32 provides QoS parameters, that would ***necessarily be before*** the relevant path is established, contrary to Patent Owner's assertions.

Pet. Reply 14 (citing Ex. 1003, 10:56–11:45; Ex. 1011 ¶ 39; Ex. 1089, 58:17–59:16; Ex. 2019, 51:21–55:6). Similarly, according to the Petition, "a person of ordinary skill in the art would have modified the VPN name server 32 of Provino to store, in part, topology dependent QoS parameters, as described by Guillen," and "[s]uch a modified VPN name server 32 would . . . respond to requests by device 12(m) to resolve the human-readable network addresses of servers 31(S) with both the integer Internet address of the servers 31(S) and the QoS parameters for the servers 31(S)." Pet. 38 (citing Ex. 1011 ¶ 43, Ex. 1005, 82, § 2.3). Petitioner adds that "one of skill would combine Guillen and Provino based on the parallel uses of DNS servers." Pet. Reply 14 (quoting Ex. 1011 ¶ 42).

At the cited paragraph, Dr. Guerin reasons that "Provino relies upon DNS servers to perform address resolution in the context of VPNs in the same manner as Guillen describes their use in the context of ATM communications." Ex. 1011 ¶ 42 (citing Ex. 1003, 10:45–67). Dr. Guerin

also relies on Guillen's disclosure of using DNS directory servers for address resolution and storing values of QoS parameters to suggest providing indications of feasible QoS levels during address resolution. Ex. 1011 ¶ 41 (citing Ex. 1005, 82, § 2.3). Dr. Guerin also cites Guillen as teaching that QoS parameters relate to guarantees such as bandwidth, and other service requirements, required for multimedia applications, so that "the multimedia application can properly function." *Id*. ¶ 40 (citing Ex. 1005, Abstract, 80–82, §§ 2.1, 2.3, 2.4).

As outlined above, the parties agree that if the modification would have been obvious, it would apply during address resolution to set up Provino's tunnel. The parties do not disagree materially, if at all, about what Guillen teaches. On balance, Guillen supports Petitioner's rationale. *See* Ex. 1005, 80–82. However, according to Patent Owner, the proposed modification of Provino's' nameserver could not work, because "by the time *Provino*'s device 12(m) accesses nameserver 32, device 12(m) and firewall 30 have <u>already</u> cooperated to establish the tunnel." PO Resp. 50.

Patent Owner's argument about "access[]" confounds the claim terms at issue, because the disputed claims require a response to include the QoS parameters. *See* PO Resp. 48 (noting that "'the response message'" [recited in claims 4, 30, and 35] refers to the message received from the secure domain name service in the independent claims"). The argument does not address Petitioner's proposed modification directly, which includes responding to device 12(m) with address information provided by nameserver 32 during Provino's set up, and providing QoS parameters that Guillen suggests to guarantee a certain level of quality for a connection, such as bandwidth. Based on the foregoing, Petitioner establishes that it would

have been obvious to respond with QoS and other parameters in a storage server, like Provino's nameserver 32, to establish the connection to server 31(s). *See* Ex. 1001, Fig. 1. "A person of ordinary skill is . . . a person of ordinary creativity, not an automaton," *KSR*, 550 U.S. at 421, and the obviousness inquiry must take account of the "routine steps" that a person of ordinary skill in the art would employ, *Ball Aerosol & Specialty Container, Inc. v. Ltd. Brands, Inc*., 555 F.3d 984, 993 (Fed. Cir. 2009).

Based on further review of the record, and for the reasons discussed above, Petitioner shows by a preponderance of evidence that the combination of Provino and Guillen renders claims 4, 6, 20, 22, 35, and 37 obvious. *See* Pet. 35–40.

C) Termination

Patent Owner argues that this proceeding should be terminated because the Board's reliance on Provino's "tunnel set up for the claimed 'access request message[]' . . . applies a rationale different from the only one proposed by Petitioner," and, therefore, the Board "exceeded its statutory authority." PO Resp. 40. Patent Owner does not contend that we relied exclusively on the Provino's "tunnel set up" scenario. *See id.* at 41 (arguing that "adopting an *additional* rationale" exceeds statutory authority) (emphasis added). As noted above (*supra* note 10), this Final Written Decision does not rely on that additional rationale, and the Institution Decision and the Final Written Decision rely on the same disclosure in Provino that Petitioner relies upon in its Petition—Provino's message packets to server 31(s). *See* Inst. Dec. 16–17; PO Resp. 39–40, 46 (arguing that packets sent to server 31(s) "might serve a different purpose entirely").

The Board has broad authority in institution decisions. *See Cuozzo*, 2015 WL 4097949, at *3–4 ("We conclude that § 314(d) prohibits review of the decision to institute IPR even after a final decision."). Patent Owner has not provided a sufficient showing to terminate the present proceeding.

III. ORDER

Petitioner has demonstrated, by a preponderance of the evidence, that Provino anticipates claims 1, 10, 12–15, 17, 26, 28–31, and 33 under 35 U.S.C. § 102; that the combination of Provino and Guillen renders claims 4, 6, 20, 22, 35, and 37 obvious under 35 U.S.C. § 103(a).

In consideration of the foregoing, it is hereby

ORDERED that claims 1, 4, 6, 10, 12–15, 17, 20, 22, 26, 28–31, 33, 35, and 37 of the '180 patent are unpatentable.

This is a final decision. Parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Jeffrey P. Kushan
Joseph A. Micallef
Scott Border
SIDLEY AUSTIN LLP
jkushan@sidley.com
jmicallef@sidley.com
sborder@sidley.com

PATENT OWNER:

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

Jason E. Stach
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
jason.stach@finnegan.com