

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION**

VIRNETX, INC.

Plaintiff

vs.

MICROSOFT CORPORATION

Defendant

§
§
§
§
§
§
§
§
§
§
§

**CASE NO. 6:07 CV 80
PATENT CASE**

MEMORANDUM OPINION

This claim construction opinion interprets the disputed terms in U.S. Patent Nos. 6,502,135 (“the ‘135 patent”); 6,839,759 (“the ‘759 patent”); and 7,188,180 (“the ‘180 patent”). Appendix A contains the disputed terms, as they appear in the asserted claims of these patents. Appendix B contains a chart summarizing the Court’s constructions.

BACKGROUND

Plaintiff VirnetX, Inc. (“VirnetX”) accuses Microsoft Corporation (“Microsoft”) of infringing claims of the ‘135, ‘759, and ‘180 patents. The ‘135 patent discloses a method of transparently creating a virtual private network between a client computer and a target computer. The ‘759 patent discloses a method for establishing a VPN without a user entering user identification information. The ‘759 patent is related to the ‘135 patent through other continuation-in-part applications/patents. The ‘180 patent discloses a method for establishing a VPN using a secure domain name service. The ‘180 patent is related to the ‘135 patent as a divisional patent of continuation-in-part applications/patents of the ‘135 patent. The ‘759 and ‘180 patents share the same specification.

APPLICABLE LAW

“It is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the invention to which the patentee is entitled the right to exclude.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In claim construction, courts examine the patent’s intrinsic evidence to define the patented invention’s scope. *See id.*; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc’ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). This intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard, Inc.*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312–13; *Alloc, Inc. v. Int’l Trade Comm’n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term’s context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can also aid in determining the claim’s meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term’s meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314–15.

“[C]laims ‘must be read in view of the specification, of which they are a part.’” *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). “[T]he specification ‘is always highly relevant to the claim construction analysis. Usually, it is dispositive;

it is the single best guide to the meaning of a disputed term.” *Id.* (quoting *Vitronics Corp. v. Conceptoronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor’s lexicography governs. *Id.* Also, the specification may resolve ambiguous claim terms “where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone.” *Teleflex, Inc.*, 299 F.3d at 1325. But, “[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.” *Comark Commc’ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *see also Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) (“As in the case of the specification, a patent applicant may define a term in prosecuting a patent.”).

Although extrinsic evidence can be useful, it is “less significant than the intrinsic record in determining the legally operative meaning of claim language.” *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard, Inc.*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid

a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition is entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

CONSTRUCTION OF DISPUTED TERMS IN THE '135 PATENT^{1,2}

"virtual private network"

The '135 patent, claims 1 and 10; the '759 patent, claims 1 and 16; and the '180 patent, claims 1, 17, and 33 contain the term "virtual private network" ("VPN"). VirnetX contends that "virtual private network" means "a network of computers capable of privately communicating with each other by encrypting traffic on insecure communication paths between the computers, and which is capable of expanding to include additional computers and communication paths." Microsoft contends that "virtual private network" means "a network implemented by encapsulating an encrypted IP packet within another IP packet (that is, tunneling) over a shared networking infrastructure." The parties dispute whether the "FreeS/WAN" dictionary may be used to construe "virtual private network," whether VirnetX's proposed construction is overly broad, whether "virtual private network" requires anonymity, and whether IP tunneling is a limitation on "virtual private network." In light of intrinsic and extrinsic evidence, the Court construes "virtual private network" as "a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers."

¹While this heading states "Construction of Disputed Terms in *the '135 Patent*," the claim terms addressed under this heading may also be found in the other asserted patents. This also applies to subsequent headings.

²Citations to the patents will not include the U.S. patent numbers to maintain brevity. Unless otherwise stated, these citations are of the U.S. patent numbers indicated in the heading that the citation falls under.

The '135 patent does not provide an explicit definition for "virtual private network." However, the '135 patent uses "virtual private network" in ways that are consistent with a "virtual private network" being "a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers." The specification discusses a VPN in the context of connecting and communicating between nodes. For instance, the specification states, "In a second mode referred to as 'promiscuous per VPN' mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network." Col. 23:11-14. This excerpt shows that the '135 invention includes nodes (computers) communicating over a virtual private network.

Furthermore, the claims and specification discuss a VPN in the context of private communication on insecure communication paths. Claim 1 states "A method of transparently creating a virtual private network (VPN) between a client computer and a target computer" and then states the steps of accomplishing this method including "requesting access to a secure web site." Col. 47:20-22, 30-31. Thus, claim 1 associates a "virtual private network" with "security." Also, the specification states, "If the user is not authorized to access the secure site, then a 'host unknown' message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site." Col. 39:21:25. This excerpt shows how a "virtual private network" establishes a secure connection between nodes where security may not otherwise exist. Thus, the claim language and the specification are consistent with construing a "virtual private network" as "a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers."

Extrinsic evidence also supports this construction. The Wiley Electrical and Electronics Engineering Dictionary defines a “virtual private network” as

A network which has the appearance, functionality, and security of a private network, but which is configured within a public network, such as the Internet. The use of a public infrastructure while ensuring privacy using measures such as encryption and tunneling protocols, helps provide the security of a private network at a cost similar to that of a public network.

WILEY ELECTRICAL AND ELECTRONICS ENGINEERING DICTIONARY 842 (2004) (published by the IEEE Press). This dictionary definition describes a network that has attributes of a private network but runs on a public network. The dictionary definition further states that encryption may be used to achieve privacy. The Court’s construction is in line with this definition. All pertinent aspects of the Court’s construction are explicitly found in the dictionary definition except for “insecure communication paths,” which simply corresponds to the dictionary definition’s reference to “a public network.” Thus, the Court’s construction is in accord with the dictionary definition.

Also, the ‘135 patent refers to the “FreeS/WAN” project in the specification. The specification explains that the “FreeS/WAN” project is developing a conventional scheme that provides secure virtual private networks over the Internet. Col. 37:50-58. The “FreeS/WAN” project defines “virtual private network” as “a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.” “FreeS/WAN” Glossary 24-25, Pl. Br. (Docket No. 194) Ex. 6. The Court’s construction is consistent with this definition.³

³The Court’s construction largely adopts VirnetX’s proposal. However, this construction excludes VirnetX’s proposed language regarding the ability of a virtual private network to expand. VirnetX proposes this language to account for the possibility of including additional computers and communication paths in a virtual private network. Pl.’s Br. 6. The Court’s construction does not limit a “virtual private network” to any particular number of computers or communication paths. Thus, VirnetX’s proposed language is superfluous. Accordingly, the Court’s construction accounts for the possibility of additional computers or communication paths.

Microsoft contends that the “FreeS/WAN” glossary is not an explicit definition of “virtual private network” and thus is not persuasive. Microsoft argues that the ‘135 patent’s reference to the “FreeS/WAN” project is made only to describe the prior art and not to define “virtual private network.” However, the specification explains that the “FreeS/WAN” project has been developing an implementation of one conventional scheme that provides secure virtual private networks over the Internet. Col. 37:50-58. Also, the applicant disclosed the “FreeS/WAN” project as prior art. *See* Def.’s Br. (Docket No. 201) Exs. M-O. While these references to the “FreeS/WAN” project do not explicitly define “virtual private network,” they at least point to extrinsic evidence that can be considered in construing “virtual private network.” Thus, the Court may consider the “FreeS/WAN” project/glossary as extrinsic evidence for construing “virtual private network.”

Microsoft also contends that even if the “FreeS/WAN” glossary offers an acceptable definition for “virtual private network,” portions of the “FreeS/WAN” glossary definition show that VirnetX’s proposed construction is overly broad. Microsoft cites the portion of the “FreeS/WAN” glossary definition for “virtual private networks” that states “IPSEC [Internet Protocol Security] is not the only technique available for building VPNs, but it is the only method defined by RFCs [Request for Comments, Internet documents—some of which are informative while others are standards] and supported by many vendors. VPNs [virtual private networks] are by no means the only thing you can do with IPSEC, but they may be the most important application for many users.” Def.’s Br. (Docket No. 201) at 10; “FreeS/WAN” Glossary 25, Pl. Br. (Docket No. 194) Ex. 6. Microsoft points out that IPSEC is the only method defined by RFCs and supported by many vendors. Microsoft argues that this narrow language shows that the “FreeS/WAN” glossary does not identify Secure Sockets Layer (“SSL”) or Transport Layer Security (“TLS”) as methods for building

“virtual private networks.” Microsoft then argues that VirnetX’s proposed construction is overly broad because it allows for a network using SSL and TLS. However, Microsoft’s cited excerpt is an ancillary portion of the “virtual private network” definition and is set apart in a different paragraph from the primary portion of the definition. *See* “FreeS/WAN” Glossary 24-25, Pl. Br. (Docket No. 194) Ex. 6. Also, Microsoft selectively asserts that IPSEC is the only method defined by RFCs and supported by many vendors and ignores that its cited excerpt states that “IPSEC is not the only technique available for building VPNs.” Thus, Microsoft’s cited excerpt does not support that the “FreeS/WAN” glossary restricts “virtual private network” to IPSEC.

Microsoft also contends that VirnetX’s proposed construction suggests that the “virtual private network” achieves only data security when it should include both data security and anonymity. Microsoft is correct that “private” in “virtual private networks” means both data security and anonymity. The specification supports this interpretation. The Background of the Invention section states “[a] tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet.” Col. 1:15-17. This section further describes data security as being “immune to eavesdropping” and states “[d]ata security is usually tackled using some form of data encryption” and anonymity as “preventing[ing] an eavesdropper from discovering that terminal 100 is in communication with terminal 110.” Col. 1:23-25, 38-39, 27-28. This language suggests that the claimed invention will achieve both data security and anonymity because it prefaces the Detailed Description of the Invention section, which describes a method of creating a virtual private network.

Indeed, the descriptions of the invention later indicate that “private” in “virtual private network” means data security and anonymity. The Detailed Description of the Invention, Further

Extensions section describes a mode of the invention as being able to “reduce the amount of overhead involved in checking for valid frames” while allowing “IP addresses . . . [to] *still be hopped* as before for secure communication within the VPN.” Col. 23:20-25 (emphasis added). The “anonymity” feature of a VPN can be handled by the Tunneled Agile Routing Protocol (“TARP”), which executes “address hopping.” *See* Col. 2:66-3:17; *see* Col. 5:49-64. Thus, the language “still be hopped” indicates that the modifications of the invention retain the anonymity feature of the “virtual private network.”⁴ Accordingly, the Court construes “virtual private network” as requiring both data security and anonymity.

Finally, Microsoft contends that “virtual private network” requires IP tunneling. Microsoft argues that the intrinsic evidence shows that TARP and IPSEC are two ways of obtaining anonymity in a virtual private network. Microsoft then argues that tunneling is required to achieve anonymity when TARP, IPSEC, or any other means is employed to achieve anonymity. The Court first and foremost considers the intrinsic evidence. The claims do not assert “tunneling” as a limitation nor has Microsoft pointed to any type of limitation in the specification. Microsoft’s citations to the Background of the Invention section only state explanations of how TARP works and does not use any limiting language. *See* Col. 3:5-18, 19-20, 58-60. Furthermore, Microsoft’s citation to the Detailed Description of the Invention, Further Extensions section only refers to a preferred implementation of the virtual private network, stating “The VPN is preferably implemented using

⁴While the specification states that this mode of the invention “[o]f course . . . compromises the anonymity of the VPNs,” this only means that those outside the VPN can discover the VPN and does not mean that the anonymity of the users within the VPN is compromised. This is clear from the example that follows the “compromising anonymity of the VPN” statement: “(i.e., an outsider can easily tell what traffic belongs in which VPN, *though he cannot correlate it to a specific machine/person*).” Col. 23:25-28 (emphasis added). Thus, the specification is consistent with construing a “virtual private network” as achieving both data security and anonymity.

the IP address ‘hopping’ features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted.” Col. 38:2-6. Again, this excerpt does not include any limiting language and in fact expressly uses the non-limiting language “preferably.” Accordingly, “virtual private network” is not limited to IP tunneling, and the Court construes “virtual private network” as “a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.”

“transparently creating [creates] a virtual private network”

The ‘135 patent, claims 1 and 10 contain the phrase “transparently creating [creates] a virtual private network.” The parties dispute whether “transparently creating a virtual private network” in the preamble is limiting and whether “transparently” refers to not involving a user or not involving the client and target computers in creating a virtual private network. VirnetX contends that this phrase means “a user need not be involved in creating a virtual private network.” Microsoft contends that the phrase does not require construction and alternatively that the phrase means “creating a virtual private network (VPN) without the client or target computer involved in requesting such creation.”

“Transparently creating a virtual private network” in the preamble is not a limitation because “transparently” does not add meaning to claims 1 and 10. “A preamble limits the invention if it recites essential structure or steps, or if it is ‘necessary to give life, meaning, and vitality’ to the claim. Conversely, a preamble is not limiting ‘where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention.’” *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002)

(citations omitted). If a preamble “is reasonably susceptible to being construed to be merely duplicative of the limitations in the body of the claim (and was not clearly added to overcome a rejection), we do not construe it to be a separate limitation.” *Symantec Corp. v. Computer Assocs. Int’l, Inc.*, 522 F.3d 1279, 1288-89 (Fed. Cir. 2008). “Transparently” is merely descriptive of what is found in steps (2) and (3) of claim 1. As discussed below, those steps require that a user is not involved in creating a VPN. This requirement corresponds to the meaning of “transparently” as described in the specification, which states that creating a VPN “is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link).” Col. 39:28-29. Thus, “transparently” is merely duplicative of what is found in the body of claim 1. As a result, the preamble is not a limitation. Accordingly, “transparently” does not require construction.

“Domain Name Service”

The ‘135 patent, claims 1 and 10 and the ‘180 patent, claims 1, 17, and 33 contain the term “Domain Name Service” (“DNS”). VirnetX contends that “Domain Name Service” means “a service that receives requests for computer network addresses corresponding to domain names, and which provides responses.” Microsoft contends that “Domain Name Service” means “the conventional lookup service defined by the Internet Engineering Task Force (“IETF”) that returns the IP address of a requested computer or host.” The parties dispute whether “Domain Name Service” is limited by the definition given in the IETF that defines Domain Name Service as the conventional scheme or if it more broadly includes both conventional and modified Domain Name Service that is described in the specification.

The specification’s description of DNS is consistent with construing DNS as “a lookup service that returns an IP address for a requested domain name.” The specification states

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

Col. 37:22-29. According to this excerpt, a DNS “provides a look-up function” and “returns the IP address of a requested computer or host.” A “computer or host” includes domain names as exemplified by the specification’s reference to “Yahoo.com” and “destination web site” as “a requested computer or host.” Accordingly, the Court construes “DNS” as “a lookup service that returns an IP address for a requested domain name.”⁵

“domain name”

The ‘135 patent, claims 1 and 10 and the ‘180 patent, claims 1, 17, and 33 contain the term “domain name.” VirnetX contends that “domain name” means “a series of characters that corresponds to an address of a computer or group of computers that is to be sent to a domain name service (DNS).” Microsoft contends that “domain name” means “a hierarchical name for a computer (such as www.utexas.edu) that the Domain Name Service converts into an IP address.” The parties dispute whether “domain name” can correspond to a group of computers or only a single computer, whether “domain name” is a hierarchical name for a computer, whether “domain name” is limited to web site names, and whether “domain name” is limited to a computer name being converted into an IP address.

The claims themselves describe “domain name.” Claim 1 states “a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer.” Col. 47:23-26. Also, claim 10 states “a DNS proxy server that receives a request from

⁵See below for the Court’s construction of “domain name.”

the client computer to look up an IP address for a domain name.” Col. 48:6-7. In both claim 1 and claim 10 an IP address corresponds to a domain name. Thus, the domain name corresponds to an IP address. Accordingly, the Court construes “domain name” as “a name corresponding to an IP address.”

VirnetX proposes that “domain name” corresponds to a group of computers (IP addresses) or a single computer because claims 1 and 10 of the ‘135 patent refer to IP address using the indefinite article “an.” The Federal Circuit has stated,

An indefinite article ‘a’ or ‘an’ in patent parlance carries the meaning of ‘one or more’ in open-ended claims containing the transitional phrase ‘comprising.’” That “a” or “an” can mean “one or more” is best described as a rule, rather than merely as a presumption or even a convention. The exceptions to [the “indefinite article”] rule are extremely limited: a patentee must “evince [] a clear intent” to limit “a” or “an” to “one.” The subsequent use of definite articles “the” or “said” in a claim to refer back to the same claim term does not change the general plural rule, but simply reinvokes that non-singular meaning. An exception to the general rule that “a” or “an” means more than one only arises where the language of the claims themselves, the specification, or the prosecution history necessitate a departure from the rule.

Baldwin Graphic Sys., Inc. v. Siebert, Inc., 512 F.3d 1338, 1342-43 (Fed. Cir. 2008) (citations omitted). Claims 1 and 10 of the ‘135 patent are open-ended construction claims using the word “comprising” and use the indefinite article “an” to refer to “IP address.” See Col. 47:20-26; see Col. 48:3-7. By the “one or more” rule, these claims allow for one or more IP addresses. Any subsequent use of the definite article “the” to refer to “IP address” simply refers back to the previously used “IP address” and thus reinvokes the non-singular meaning. See Col. 47:39-40; see Col. 48:8. Microsoft does not assert any evidence to show that an exception to the “one or more” rule exists. Thus, there may be more than one IP address, and thus more than one computer, that corresponds with the domain name. This would allow for a situation where the IP address that corresponds to the domain

name is not the IP address of the target computer. *See* Col. 38:23-42. Accordingly, “domain name” can correspond to more than one computer.

Microsoft contends that the patents limit “domain name” to a hierarchical name for a computer under traditional hierarchical DNS format. However, Microsoft relies largely on extrinsic evidence—including expert testimony and Microsoft’s own technology tutorial—to support its contentions, which does not carry great weight in light of the fact that claim language provides guidance on the meaning of “domain name.” Also, where Microsoft uses intrinsic evidence for support, Microsoft only refers to non-limiting language from the specification. For instance, Microsoft suggests that the examples used in the specification for domain names, which include “Yahoo.com” and “Target.com,” show that the patents use “domain name” in its traditional hierarchical DNS format. Microsoft further suggests that “domain name” is limited to a traditional hierarchical name because the patents do not provide a single example of “domain name” that is not written in traditional hierarchical DNS format. However, Microsoft argues only the presence and absence of examples rather than any enforceable language of limitation. The specification’s disclosure or omission of examples does not create limitations on claims. Accordingly, Microsoft does not offer sufficient support for limiting “domain name” to a hierarchical name for a computer.

Microsoft also contends that the patents limit “domain name” to web site names. However, no such limitation is found in the claims, and Microsoft merely references its arguments on construing “web site” without showing how “domain name” is necessarily linked to web site names. Accordingly, “domain name” is not limited to web site names.

Finally, Microsoft contends that “domain name” is limited to a computer name being converted into an IP address. Microsoft supports this proposed limitation by arguing that a “domain

name” has the capacity to be converted by DNS into an IP address and that the specification emphasizes this point by describing that identical DNS requests may result in conventional domain name resolution, “host unknown” error messages, or VPN initiation, depending not on whether something is a “domain name” but on what type of web site was requested. However, Microsoft incorrectly argues that a “capacity” to be converted by DNS into an IP address demonstrates a required limitation. A mere capacity to perform an act does not make that act necessary. Thus, Microsoft has not sufficiently supported limiting “domain name” to a computer name being converted into an IP address. Accordingly, the Court construes “domain name” as “a name corresponding to an IP address.”

“web site”

The ‘135 patent, claims 1 and 10 contain the term “web site.” VirnetX contends that construing “secure web site” as addressed below sufficiently addresses the meaning of “web site” and that “web site” does not require further construction. Alternatively, VirnetX contends that “web site” means “a computer associated with a domain name and that can communicate in a network.” Microsoft contends that “web site” means “one or more related web pages at a location on the World Wide Web.” The parties dispute whether “web site” should be given a construction separate from “secure web site” and whether “web site” is limited to web pages on the World Wide Web.

VirnetX argues that “web site” should not be construed separately from “secure web site” because the ‘135 patent claims never state “web site” without the preceding word “secure.” However, “secure” is separable from “web site” as a modifier of “web site.” The claims show that “secure” can be replaced by other modifiers to “web site.” Claims 1 and 10 of the ‘135 patent refer to “web site” preceded by “non-secure” and “secure target.” Col. 47:28, 30; Col. 48:10, 14. This

demonstrates that “web site” can be separated from its modifier and thus is its own term separate from “secure.” Thus, “web site” may be construed as its own claim term.

The Court adopts Microsoft’s construction and construes “web site” as “one or more related web pages at a location on the World Wide Web.” The patent does not state a definition for “web site.” However, the term itself is instructive. “Web site” on its face refers to a “web” Internet resource, which is a web page on the World Wide Web. The specification is consistent with construing “web site” as a web page on the World Wide Web. Examples of web sites in the specification are “Yahoo.com” and “Target.com.” Col. 37:25, 45. “Yahoo.com” and “Target.com” are well-known web pages on the World Wide Web. *See* Yahoo! Home Page, www.Yahoo.com; *see* Target Home Page, www.Target.com. Also, the specification states that a “web browser” can be used to access a “web site.” Col. 39:48, 50-51, 55; Col. 40:1, 38. It is well-known that a “web browser” is used to navigate “web pages” on the World Wide Web. Thus, the intrinsic evidence supports Microsoft’s proposed construction.

Furthermore, extrinsic evidence supports Microsoft’s construction. The World Wide Web Consortium, an industry standards-setting organization for the World Wide Web, defined web site as “[a] collection of interlinked Web pages, including a host page, residing at the same network location.” Brian Lavoie & Henrik Frystyk Nielsen, *Web Characterization Terminology & Definitions Sheet, W3C Working Draft* (May 24, 1999) at 9, Def.’s Resp. (Docket No. 201), Ex. X (emphasis removed). This definition is consistent with industry dictionaries, which define a web site as “A collection of logically connected Web pages managed as a single entity” and “A group of HTML documents and associated scripts supported by a Web server on the World Wide Web.” *AUTHORITATIVE DICTIONARY OF IEEE STANDARDS TERMS* 1276 (7th ed. 2000), Def.’s Resp.

(Docket No. 201) Ex. Y; DICTIONARY OF NETWORKING 404 (3d ed. 1999), Def.'s Resp. (Docket No. 201) Ex. H. Accordingly, the Court construes "web site" as "one or more related web pages at a location on the World Wide Web."

VirnetX proposes construing "web site" as "a computer associated with a domain name." This construction would broaden the meaning of "web site" beyond how this term is used in the patent. VirnetX's construction does not include the limitations "web page" and "World Wide Web." Without these limitations, the claims would include a right to exclude over computers with network addresses that do not host web pages. This would offend the meaning of the claim term itself. "*Web site*" on its face requires a site on the World Wide Web. The patentee chose to use "web site" in the claims instead of using a more encompassing term like "host," "target computer," or "Internet resource." Thus, the patentee cannot gain broader claim protection from what he disclosed to the public as "web site."

VirnetX contends that the specification demonstrates a broader meaning of "web site" than what Microsoft proposes. VirnetX argues that the specifications refers to "web site" as "host," which suggests that "web site" carries the broader meaning of "host." However, the claims and not the specification define the scope of the right to exclude. *See Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1248 (Fed. Cir. 1998) ("the claims define the scope of the right to exclude; the claim construction inquiry, therefore, begins and ends in all cases with the actual words of the claim") (citation omitted). The patentee chose to use "web site" in the claims and thus the claims are limited by that term. Accordingly, the Court construes "web site" as "one or more related web pages at a location on the World Wide Web."

“secure web site”

The ‘135 patent, claims 1 and 10 contain the term “secure web site.” VirnetX contends that “secure web site” means “a computer associated with a domain name and that can communicate in a virtual private network.” Microsoft contends that “secure web site” means “web site that requires authorization for access.” The parties dispute whether a “secure web site” requires authorization for access and whether a “secure web site” can communicate in a virtual private network.

The Court has construed “web site.” *See supra*. The Court construes “secure web site” as “a web site that requires authorization for access and that can communicate in a VPN.” First, the specification supports that a “secure web site” “requires authorization for access.” The specification states

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 communication services 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 of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. *For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently “passes through” the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites.* Different users who make an identical DNS request could be provided with different results.

Col. 37:63-38:13 (emphasis added). These italicized portions explain that “secure” relates to registered users who have the ability to set up a virtual private network with a target node. This supports that “secure” means “requiring authorization for access.”⁶

⁶While the specification uses “e.g.” in the cited excerpt above, the Court’s reasoning does not rely on the portions designated as examples.

Second, the claims themselves support that a “secure web site” “can communicate in a VPN.” Claims 1 and 10 state “transparently creating [create] a virtual private network (VPN) between a client computer and a target computer.” Col. 47:20-22; Col. 48:3-5. The “client computer” may seek access to a “secure target web site,” which is on the target computer. *See* Col. 47:20-22; Col. 48:3-5. Because a VPN may be established between the client computer and target computer, the “secure target web site” can communicate in the VPN so that the client computer can access the “secure target web site” at the target computer. *See* Col. 47:29-32; *see* Col. 48:16-19. Accordingly, a “secure web site” “can communicate in a VPN,” and the Court construes “secure web site” as “a web site that requires authorization for access and that can communicate in a VPN.”

“determining whether the DNS request transmitted in step (1) is requesting access to a secure web site”

The ‘135 patent, claim 1 contains the phrase “determining whether the DNS request transmitted in step (1) is requesting access to a secure web site.” VirnetX contends that this phrase does not require construction. Alternatively, VirnetX contends that the phrase means “determining whether the DNS request transmitted in step (1) is requesting VPN communication with a secure web site.” Microsoft contends that the phrase means “the computer receiving the DNS request checks the request to determine whether access to a secure web site was requested.” The parties dispute whether the phrase at issue requires a construction, and if so, what performs the determining step.

No construction is necessary beyond the terms already construed in the phrase “determining whether the DNS request transmitted in step (1) is requesting access to a secure web site.” The Court has construed “DNS” and “secure web site.” “Determining whether the . . . transmitted in step

(1) is requesting access to a” has an ordinary meaning that a jury would understand without construction. Accordingly, the Court does not construe “determining whether the DNS request transmitted in step (1) is requesting access to a secure web site.”

However, the parties dispute whether “determining whether the DNS request transmitted in step (1) is requesting access to a secure web site” must be performed by the computer receiving the DNS request. Microsoft argues that it does not make sense for the client computer to generate a DNS request as stated in step 1 and then perform the subsequent “determining” step in step 2. VirnetX argues that nothing in the claim limits which computers perform the “determining” step. VirnetX also argues that there are circumstances where a client computer may have one program that transmits the DNS request to a second program on the same client computer, and the second program performs the “determining” step on the same client computer. Finally, VirnetX argues that the doctrine of claim differentiation between claims 1 and 2 of the ‘135 patent shows that the “determining” step may be performed by the client computer.

The client computer can perform the “determining” step. Nothing in claim 1 of the ‘135 patent prevents the client computer from “determining whether the DNS request transmitted in step (1) is requesting access to a secure web site.” *See* Col. 47:20-32. Also, the doctrine of claim differentiation shows that the client computer may perform the “determining” step. Courts presume a difference in meaning and scope when a patentee uses different phrases in separate claims. *Phillips*, 415 F.3d at 1314–15. Claim 2 states “The method of claim 1, wherein steps (2) and (3) are performed at a DNS server *separate from the client computer*.” Col. 47:33-35 (emphasis added). Claim 2 states the limitation “separate from the client computer” whereas claim 1 does not. Thus, presumably this limitation is not found in claim 1. This presumption cannot be rebutted because

there is no language in claim 1 that limits the “determining” step to computers other than the client computer. Accordingly, “determining whether the DNS request transmitted in step (1) is requesting access to a secure web site” is not limited to being performed by the computer that receives the DNS request.

“automatically initiating the VPN”

The ‘135 patent, claim 1 contains the phrase “automatically initiating the VPN.” VirnetX contends that “automatically initiating the VPN” means “starting the VPN without intervention by a person.” Microsoft contends that “automatically initiating the VPN” means “initiating the VPN without the client or target computer requesting such initiation.” The parties dispute whether “automatically” refers to not requiring a user or refers to not requiring the client and target computers.

The Court construes “automatically initiating the VPN” as “initiating the VPN without involvement of a user.” The specification supports the Court’s construction. The specification describes various embodiments of the invention. *See* Col. 37:63-40:13. In these embodiments, after the user or user’s computer makes the initial DNS request, the user is not further involved in setting up the VPN. *See, e.g.*, Col. 39:22-29 (describing that if the user has sufficient security privileges, a secure VPN is established between the user’s computer and the secure target website “preferably performed transparently to the user (i.e. the user need not be involved in creating the secure link)”; 38:28-33 (describing that the DNS proxy 2610 determines whether the user has sufficient security privileges to access the required site and if so, the “DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between a user computer 2601 and secure target site 2604”); Figs. 26 & 27. Thus, the specification describes that the VPN is

initiated without further user action.

Microsoft argues that “automatically” does not refer to a “user” because claim 1 does not make any reference to a person and instead states “automatically initiating the VPN between the client computer and the target computer.” Col. 47:20-32. Microsoft concludes that claim 1 clearly refers to not involving the client and target computers when stating “automatically.” However, claim 1 only refers to the client and target computers to indicate where the VPN is being established, “between the client computer and the target computer.” This phrase does not disallow involvement of the client and target computers in initiating the VPN. Instead, as discussed *supra*, the specification shows that “automatically” refers to not involving a user.

Furthermore, the difference between independent claim 1 and dependent claim 2 indicates that the client computer can be involved in step (3) of claim 1, which includes “automatically initiating the VPN.” Claim 2 states “The method of claim 1, wherein steps (2) and (3) are performed at a DNS server *separate from the client computer*.” Col. 47:33-35 (emphasis added). Because claim 2 contains “separate from the client computer” and claim 1 does not, claim 1 presumably does not contain this limitation. This claim differentiation presumption is not rebutted in light of the intrinsic evidence. Thus, the client computer may be involved in initiating the VPN in claim 1. Accordingly, the Court does not adopt Microsoft’s construction, but construes “automatically initiating the VPN” as “initiating the VPN without involvement of a user.”

“DNS proxy server”

The ‘135 patent, claim 10 contains the term “DNS proxy server.” VirnetX contends that “DNS proxy server” means “a computer or program that responds to a domain name inquiry in place of a DNS.” Microsoft contends that “DNS proxy server” means “a computer that intercepts a DNS

request from a client computer to a DNS server and checks the request to determine whether access to a secure web site has been requested.” The parties dispute whether the “DNS proxy server” must check the DNS request or if it “responds” to a domain name inquiry, whether “DNS proxy server” can only be a computer or if it can be a computer or a program, and whether the “DNS proxy server” must be separate from the client computer.

The Court adopts VirnetX’s proposed construction and construes “DNS proxy server” as “a computer or program that responds to a domain name inquiry in place of a DNS.” First, the claim language supports that a “DNS proxy server” “responds to a domain name inquiry in place of a DNS.” Claim 10 states

a DNS proxy server that *receives a request* from the client computer to look up an IP address for a domain name, wherein the *DNS proxy server returns the IP address* for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the *DNS proxy server generates a request* to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested.

Col. 48:6-15 (emphasis added). This excerpt shows that a DNS proxy server receives a request from the client computer to look up an IP address for a domain name and then responds by returning the IP address for the requested domain name or by creating a VPN, depending on the type of request made by the client computer. Thus, a DNS proxy server “responds” according to the type of request made by the client computer.

Second, the specification supports that the “DNS proxy sever” is a “computer or program.” The specification discusses a “DNS proxy server” in the following context: “It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience. Moreover, although element 2602 is shown as combining the functions of two

servers, the two servers can be made to operate independently.” Col. 38:61-65. This excerpt discusses a DNS proxy server as potentially being combined into a single server, and those skilled in the art understand “servers” as including computers. *See* IEEE 100: THE AUTHORITATIVE DICTIONARY OF IEEE STANDARDS TERMS 1031 (7th ed. 2000) (defining “server” in the third definition as “In a network, a device or computer system that is dedicated to providing specific facilities to other devices attached to the network”). Then, the specification discusses “combining the functions of two servers.” Functions on servers/computers are understood by those skilled in the art to be controlled by software. Thus, the specification discusses a “DNS proxy server” as a “computer or program.” Accordingly, the Court construes “DNS proxy server” as “a computer or program that responds to a domain name inquiry in place of a DNS.”

Finally, Microsoft seeks to limit “DNS proxy server” to being separate from the client computer. Microsoft argues that the “DNS proxy server” must be separate from the client computer because the claim language discloses “a DNS proxy server that receives a request from the client computer.” Col. 48:6-7. Microsoft contends that this language cannot be consistent with VirnetX’s proposed construction that allows for a program on the client computer to send a DNS request to another program on the same computer. However, Microsoft’s cited language does not limit a “DNS proxy server” from being a part of the client computer. Microsoft’s cited language only states that the DNS proxy server receives a request from the client computer without further limiting that the DNS proxy server cannot be a part of the client computer. Accordingly, the “DNS proxy server” does not have to be separate from the client computer.

CONSTRUCTION OF DISPUTED TERMS IN THE '759 PATENT

“secure communication link”

The '759 patent, claims 1 and 16 contain the term “secure communication link.” VirnetX contends that “secure communication link” means “virtual private network communication link.” Microsoft contends “secure communication link” means “encrypted communication link.”

No construction is necessary for “secure communication link.” The claim language itself defines “secure communication link.” Claims 1 and 16 state “the secure communication link being a virtual private network communication link.” Col. 57:20-22; Col. 58:311-33. Given that the claims themselves define “secure communication link,” no construction is necessary.

“the secure communication link being a virtual private network communication link”

The '759 patent, claims 1 and 16 contain the phrase “the secure communication link being a virtual private network communication link.” VirnetX and Microsoft agree that this phrase does not require construction.

“virtual private network communication link”

The '759 patent, claims 1 and 16 and the '180 patent, claims 1, 17, 33 contain the term “virtual private network communication link.” VirnetX contends that “virtual private network communication link” means “a communication path between computers in a virtual private network.” Microsoft contends that “virtual private network communication link” means “communication link in a virtual private network.”

The Court has construed “virtual private network.” *See supra*. Also, “communication” and “link” are common terms that jurors would understand without a claim construction, and the patents do not assign any specialized meaning to these terms. Accordingly, the Court does not construe

“virtual private network communication link.”

VirnetX argues that the “virtual private network communication link” is the entire communication path between computers in a virtual private network. VirnetX cites to various parts of the specification that state that a communication link is between computers “over a [the] computer network.” *See* ‘759 patent, Abstract; 6:63-65; 50:50-64; 51:45-47; 53:38-42; 53:48-55. VirnetX then argues that “over a computer network” means over the “entire” computer network. However, VirnetX’s cited excerpts of the specification only state “over a computer network” and not over an “entire” computer network or anything resembling such encompassing language. The claim language does not state anything to this extent either. Accordingly, the Court does not limit “virtual private network communication link” to being over the entire computer network.

“enabling a secure communication mode of communication at the [a] first computer without a user entering any cryptographic information for establishing the secure communication mode of communication”

The ‘759 patent, claims 1 and 16 contain the phrase “enabling a secure communication mode of communication at the [a] first computer without a user entering any cryptographic information for establishing the secure communication mode of communication.” VirnetX contends that this phrase means “providing to the first computer at least one resource necessary for a virtual private network communication, based on a domain name service (DNS) that provides the resource according to user identity, without user input of encoding or decoding information.” Microsoft contends that the phrase does not require construction. Alternatively, Microsoft contends that only “cryptographic information” requires construction and means “information used for encryption.” The parties dispute whether construction is necessary, and if construction is necessary, what limitations to apply.

The only term that requires construction in “enabling a secure communication mode of communication at the [a] first computer without a user entering any cryptographic information for establishing the secure communication mode of communication” is “cryptographic information” as a jury may not understand the meaning of “cryptographic.” VirnetX argues that “cryptographic information” is encoding or decoding information. Microsoft argues that “cryptographic information” is information used for encryption. Microsoft contends that “encoding or decoding” is too broad because all information stored on a computer or transmitted over the Internet is encoded or decoded. VirnetX contests that “encryption” is too narrow because “encryption” does not account for the “decryption” aspect of “cryptographic information.”

The Court construes “cryptographic information” as “information that is encoded/decoded or encrypted to ensure secrecy.” This construction addresses both VirnetX’s request to use “encoding or decoding” and Microsoft’s request to use “encryption” to construe “cryptographic information.” Also, Microsoft’s concern that “encoding or decoding” is too broad because all information is encoded and decoded is addressed by the Court’s construction language “to ensure secrecy,” which modifies both “encoded/decoded” and “encrypted.” Additionally, extrinsic evidence is consistent with the Court’s construction. “Cryptographic” is defined as “in an encrypted form; using a code or cipher.” ACADEMIC PRESS DICTIONARY OF SCIENCE AND TECHNOLOGY 556 (1992) (second definition). This supports the most limiting portion of the Court’s construction that states “cryptographic information” is information that is “encrypted.”

VirnetX contends that the additional terms—“enabling,” “establishing,” and “secure communication mode of communication”—require construction. VirnetX argues that these terms require constructions because they do not by themselves explain how the claimed invention is

carried out. However, the claims do not need to state how to perform the claimed invention. *See SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1121 n.14 (Fed. Cir. 1985) (“Specifications teach. Claims claim.”). Limitations from the specification do not have to be imported just because the claims do not state how to perform the invention. Furthermore, VirnetX’s citations describe only particular aspects and embodiments. *See* Pl.’s Br. (Docket No. 194) at 34; *see* Col. 6:37, 44. “Although the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.” *Comark*, 156 F.3d 1182, 1187. Accordingly, the Court does not adopt VirnetX’s proposed limitations and construes only “cryptographic information” as “information that is encoded/decoded or encrypted to ensure secrecy.”

CONSTRUCTION OF DISPUTED TERMS IN THE ‘180 PATENT

“secure computer network address”

The ‘180 patent, claims 1, 17, and 33 contain the term “secure computer network address.” VirnetX contends that “secure computer network address” means “a network address associated with a computer capable of virtual private network communications.” Microsoft contends that “secure computer network address” means “a network address that requires authorization for access.” The parties dispute whether the network address “requires authorization for access.”

The Court construes “secure computer network address” as “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.” First, the claim language supports that the network address requires authorization for access. Claim 1 of the ‘180 patent states “[a] method for accessing a secure computer network address, comprising the steps of.” Col. 56:48-50. The claim then goes on to list

the method steps including “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.” Col. 56:55-57; 56:58-59. This supports that the “secure computer network address” requires authorization because there must be a request made to the “secure computer network address” in order to access the “secure computer network address.” Accordingly, the Court uses “requires authorization for access” in construing “secure computer network address.”

Second, the claim language supports that a “secure computer network address” is associated with a computer capable of virtual private network communications. Claim 1 states “A method for accessing a secure computer network address, comprising steps of,” Col. 56:48-50. The claim later states the step “sending an access request message to the secure computer network address using a virtual private network communication link.” Col. 56:59-61. Thus, the secure computer network address receives an access request message via a virtual private network communication link. This shows that the secure computer network address is associated with the computer at the secure computer network address that is using the virtual private network communication link. Accordingly, the Court construes “secure computer network address” as “a network address that requires authorization for access and is associated with a computer capable of virtual private network communications.”

“secure domain name”

The ‘180 patent, claims 1, 17, and 33 contain the term “secure domain name.” VirnetX contends that “secure domain name” means “a domain name which indicates that it is to be translated into a secure computer network address by a secure domain name service.” Microsoft

contends that “secure domain name” means “a non-standard top-level domain name (such as .scom, .sgov. or .sorg) that corresponds to a secure computer network address.” The parties dispute whether the claimed invention is limited to “non-standard top-level domain name.”

The Court construes “secure domain name” as “a domain name that corresponds to a secure computer network address.” “Secure domain name” ordinarily includes “non-standard top-level” domain names or equivalents as suggested by the specification, but “non-standard top-level” is not a limitation. Claim differentiation shows that “secure domain name” is not limited to “non-standard top-level” domain names. Differences among the claim terms can assist in understanding a term’s meaning. *Phillips*, 415 F.3d at 1314. For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314–15. Dependent claims 11, 27, and 41 contain the “top-level” limitation whereas their corresponding independent claims 1, 17, and 33 do not. Thus, it is presumed that independent claims 1, 17, and 33 do not contain the “top-level” limitation. As a result, “secure domain name,” without further express limitations provided in the claims, presumably does not contain the “top-level” limitation.

Microsoft argues that there is clear disavowal in the specification. The specification states

The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network address for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

Col. 7:36-42 (emphasis added). Thus, the specification asserts that the invention provides the secure domain names that are “non-standard top-level,” using the “present invention” language. However, such language is not necessarily limiting. “Use of the phrase ‘the present invention’ does not ‘automatically’ limit the meaning of claim terms in all circumstances, and . . . such language must be read in the context of the entire specification and prosecution history.” *Netcraft Corp. v. eBay, Inc.*, 549 F.3d 1394, 1398 (citing *Rambus Inc. v. Infineon Techs. AG*, 318 F.3d 1081, 1094 (Fed. Cir. 2003)). The claims show that “non-standard top-level” should not be imported as a limitation into the claims. Accordingly, the Court does not use “non-standard top-level” in construing “secure domain name.”

There is no dispute as to whether “secure domain name” “corresponds to a secure computer network address.” In any case, the claim language itself states that a secure domain name corresponds to a secure computer network address. Claim 1 states “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.*” Col. 56:51-55 (emphasis added). Thus, the claim language clearly establishes that a secure domain name corresponds to a secure computer network address. Accordingly, the Court construes “secure domain name” as “a domain name that corresponds to a secure computer network address.”

“secure domain name service”

The ‘180 patent, claims 1, 17, and 33 contain the term “secure domain name service.” VirnetX contends that “secure domain name service” means “a service that receives requests for secure computer network addresses corresponding to secure domain names, and is capable of providing trustworthy responses.” Microsoft contends “secure domain name service” means “a

domain name service that provides secure computer network addresses for secure, non-standard top-level domain names.”

The Court construes “secure domain name service” as “a lookup service that returns a secure network address for a requested secure domain name.” This construction is consistent with the claim itself. Claim 1 states

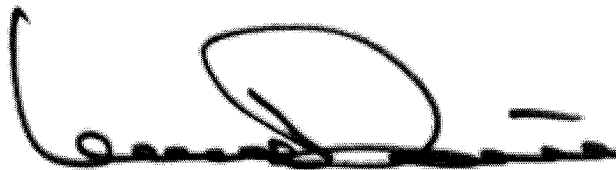
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name; receiving from the secure domain name service a response message containing the secure computer network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

Col. 56:51-61. This language shows that the secure domain name service receives a query message requesting a secure computer network address that corresponds to a secure domain name. Then, the secure domain name service sends a response message containing the secure computer network address that corresponds to the requested secure domain name. As such, the secure domain name service looks up a secure domain name network address in response to a requested secure domain name. Accordingly, the Court construes “secure domain name service” as “a lookup service that returns a secure network address for a requested secure domain name.”

CONCLUSION

For the foregoing reasons, the Court interprets the claim language in this case in the manner set forth above. For ease of reference, the Court’s claim constructions are set forth in a table in Appendix B. The disputed claims with the disputed terms in bold are set forth in Appendix A.

So ORDERED and SIGNED this 30th day of July, 2009.

A handwritten signature in black ink, appearing to read 'Leonard Davis', with a large, stylized loop at the end.

LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPENDIX A

U.S. Patent No. 6,502,135

1. A method of **transparently creating a virtual private network (VPN)** between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a **Domain Name Service (DNS)** request that requests an IP address corresponding to a **domain name** associated with the target computer;

(2) **determining whether the DNS request transmitted in step (1) is requesting access to a secure web site;** and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target **web site**, **automatically initiating the VPN** between the client computer and the target computer.

10. A system that **transparently creates a virtual private network (VPN)** between a client computer and a secure target computer, comprising:

a **DNS proxy server** that receives a request from the client computer to look up an IP address for a **domain name**, wherein the **DNS proxy server** returns the IP address for the requested **domain name** if it is determined that access to a non-secure **web site** has been requested, and wherein the **DNS proxy server** generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a **secure web site** has been requested; and

a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the **DNS proxy server**.

U.S. Patent No. 6,839,759

1. A method for establishing a **secure communication link** between a first computer and a second computer over a computer network, the method comprising steps of:

enabling a secure communication mode of communication at the first computer without a user entering any cryptographic information for establishing the secure communication mode of communication; and

establishing the **secure communication link** between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication, the **secure communication link being a virtual private network communication link** over the computer network.

16. A computer-readable storage medium, comprising: a storage area; and

computer-readable instructions for a method for establishing a **secure communication link** between a first computer and a second computer over a computer network, the method comprising steps of:

enabling a secure communication mode of communication at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication; and

establishing a **secure communication link** between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication, the **secure communication link being a virtual private network communication link** over the computer network.

U.S. Patent No. 7,188,180

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**.

17. A computer-readable storage medium, comprising:

a storage area; and

computer-readable instructions for a method for accessing a **secure computer network address**, the method comprising steps of:

receiving a **secure domain name**;

sending a query message to a **secure domain name service**, the query message requesting from the **domain name service** a **secure computer network address** corresponding to the **secure domain name**;

receiving from the **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**.

33. A data processing apparatus, comprising:

a processor, and

memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a **secure computer network address**, said method 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**.

APPENDIX B

| Term | Definition |
|--|--|
| virtual private network | a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers |
| transparently creating [creates] a virtual private network (VPN) | [no construction necessary] |
| Domain Name Service (DNS) | a lookup service that returns an IP address for a requested domain name |
| domain name | a name corresponding to an IP address |
| web site | one or more related web pages at a location on the World Wide Web |
| secure web site | a web site that requires authorization for access and that can communicate in a VPN |
| determining whether the DNS request transmitted in step (1) is requesting access to a secure web site | [no construction necessary] |
| automatically initiating the VPN | initiating the VPN without involvement of a user |
| DNS proxy server | a computer or program that responds to a domain name inquiry in place of a DNS |
| secure communication link | [no construction necessary] |
| the secure communication link being a virtual private network communication link | [no construction necessary] |
| virtual private network communication link | [no construction necessary] |
| cryptographic information in the phrase "enabling a secure communication mode of communication at the [a] first computer without a user entering any cryptographic information for establishing the secure communication mode of communication" | information that is encoded/decoded or encrypted to ensure secrecy |
| secure computer network address | a network address that requires authorization for access and is associated with a computer capable of virtual private network communications |
| secure domain name | a domain name that corresponds to a secure computer network address |
| secure domain name service | a lookup service that returns a secure network address for a requested secure domain name |