

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:)
Victor Larson et al.) Control No.: 95/001,788
U.S. Patent No. 7,418,504) Group Art Unit: 3992
Issued: August 26, 2008) Examiner: Roland Foster
For: AGILE NETWORK PROTOCOL FOR SECURE) Confirmation No.: 5823
COMMUNICATIONS USING SECURE)
DOMAIN NAMES)

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

PATENT OWNER'S RESPONSE TO
OFFICE ACTION OF SEPTEMBER 26, 2012

On December 29, 2011, the U.S. Patent and Trademark Office ("Office") issued a first Office Action ("First OA" or "First Office Action") in these reexamination proceedings. VirnetX Inc. ("VirnetX" or "Patent Owner"), the owner of U.S. Patent No. 7,418,504 ("the '504 patent"), filed a Response ("Response") on March 29, 2012. Requester Apple Inc. ("Apple" or "Requester") filed Comments ("Comments") on June 25, 2012. On September 26, 2012, the Office issued a second Office Action ("Second OA" or "Second Office Action"), which was an Action Closing Prosecution ("ACP"), in these proceedings.

Claims 1-60 are patentable at least for the reasons that follow and the reasons stated in VirnetX's March 29 Response. Thus, VirnetX requests that claims 1-60 be confirmed. This Response is supported by a Supplemental Declaration of Angelos D. Keromytis, Ph.D. ("Supp. Keromytis Decl."). At times, this Response also refers to the initial Declaration of Angelos D. Keromytis, Ph.D. ("Keromytis Decl.") supporting the Response filed on March 29, 2012.

I. The Rejections Are Based on Improper Claim Constructions

The Office's patentability conclusions are defective because the Office takes incorrect positions on claim construction. In some instances, the Office proposes unreasonably broad constructions, stretching the '504 patent claims beyond their proper scope to read on the asserted references. In other instances, the Office advocates constructions that are inconsistent with clear

disclaimers in the '504 patent specification. Still in others, the Office does not apply the claim construction it elsewhere purports to adopt. These are effectively new claim-construction positions taken in the ACP, which Patent Owner has not had a chance to rebut. Given these new positions advocated by the Office, the latest Office Action should not have been an ACP.¹ See M.P.E.P. § 2671.02 (“Before an ACP is in order, a clear issue should be developed.”). Moreover, as explained below, even under the new positions raised in the ACP, the Office has not demonstrated that the claims are unpatentable.

A. Standards for Claim Construction

“During reexamination, claims are given the broadest reasonable interpretation consistent with the specification” *Id.* § 2258(I)(G); *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1148 (Fed. Cir. 2012). But while “the USPTO must give claims their broadest reasonable interpretation in light of the Specification,” this does not mean that it may construe a claim term to have an atypical meaning. *In re Kuibira*, Appeal No. 2009-002409, 2010 WL 390100, at *2 (B.P.A.I. Feb. 1, 2010). Instead, “the words of the claim must be given their *ordinary* meaning unless the ordinary meaning is inconsistent with the Specification.” *Id.* (emphasis added). As the Board noted, “the purpose [of giving claims their broadest reasonable interpretation] is not to stretch the interpretation of a claim limitation beyond what would be reasonably understood by the skilled worker in the light of the Specification, to read on a prior art structure which could possibly, but not reasonably, be covered by it.” *In re Alferness*, Appeal No. 2009-0122, 2009 WL 1171349, at *6 (B.P.A.I. Apr. 30, 2009). Given the Federal Circuit’s and the Board’s focus on reading claims in light of the specification, the Examiner is not free to disregard plain statements in the specification disclaiming certain embodiments from the scope of the claimed invention.

B. The Rejections Are Based on Incorrect Constructions of the Claimed “Domain Name Service System”

Independent claim 1 recites “a *domain name service system* configured to . . . comprise an indication that the *domain name service system* supports establishing a secure communication link” (emphases added). Independent claims 36 and 60 also recite a “domain name service system.” Accordingly, every claim of the '504 patent expressly recites, or incorporates by virtue of its dependency, features relating to a “domain name service system” (“DNS system”). (See '504 patent

¹ The Second Office Action should not have been an ACP, so Patent Owner requests a new, nonfinal Office Action for at least the reasons discussed in Patent Owner’s Petition to Reopen Prosecution Pursuant to 37 C.F.R. § 1.181, filed November 26, 2012.

55:49-60:14.) The Office’s construction of the claimed “DNS system,” however, is unreasonably broad.

In construing “DNS system,” the Office states that a DNS system can include a single “DNS device” or multiple “DNS devices.” (Second OA at 15-18, referring to sections of the ’504 patent that discuss the roles of gatekeeper 2603, DNS proxy 2610, and DNS server 2609.) The Office then stretches this understanding to contend that virtually any device—regardless of whether it has any DNS functionality—may be a “DNS device” as long as it is in the same network as at least one device that actually has DNS functionality. Indeed, the Office construes a “DNS system” and interprets a “DNS device” as having no bounds whatsoever, and it applies those terms accordingly. (*See id.*)

Through these improper constructions, the Office has stretched the recited DNS system beyond its proper scope to encompass, in the asserted references, many devices that one of ordinary skill in the art would have viewed as *non-DNS* devices, *outside* the scope of a DNS system. (Supp. Keromytis Decl. ¶¶ 8-9.) For example, the Office contends devices like firewalls, key exchanger nodes, client and server devices, and other devices performing no DNS functions whatsoever are part of the claimed DNS system. If the Office’s unbounded view of a DNS device is correct, virtually *any* component, if connected to a computing network that has DNS functionality somewhere within it (e.g., the Internet), qualifies as a DNS device within a DNS system. (*Id.* ¶ 9.) The Office’s construction is simply unreasonably broad and is inconsistent with how one of ordinary skill in the art would have understood a DNS system, particularly in light of the ’504 patent specification.

The Office relies on the ’504 patent’s description of gatekeeper 2603, DNS proxy 2610, and DNS server 2609 to support its unreasonable interpretation of a DNS system. However, the ’504 patent discloses significant DNS functionality and coordination between these devices in acting upon a DNS request. (*Id.* ¶¶ 6-7.) For example, the ’504 patent specification explains that, in one scenario, DNS proxy 2610 receives a DNS request, determines that the DNS request is for a nonsecure target site, and passes the DNS request through to DNS server 2609 for resolution to the client. (’504 patent 40:6-8, 40:25-29, 40:53-56.) Thus, DNS proxy 2610 and DNS server 2609 interact with each other to process a DNS request, and the client need not run separate lookups with both the proxy and the server. (*Id.*; Supp. Keromytis Decl. ¶ 7.) Alternatively, DNS proxy 2610 may determine that the DNS request is for a secure target site, perform an authorization check, transmit a message to gatekeeper 2603 to facilitate creating a VPN link, and obtain a resolved address from the gatekeeper 2603 to return to the client. (’504 patent 40:6-24, 40:57-59.) Again, in this scenario, the DNS proxy 2610 and the gatekeeper 2603 interact together to process a DNS request, and the client

need not run separate lookups with the proxy and the gatekeeper. (*Id.*; Supp. Keromytis Decl. ¶ 7.) These devices all have significant DNS functionality, and any assertion that DNS devices may include devices not having actual DNS functionality directly contradicts the explicit and consistent teachings of the '504 patent specification. By doing just this, the Office adopts an unreasonable construction of a DNS system with no outer limits that sweeps in non-DNS devices. (Supp. Keromytis Decl. ¶¶ 8-9.) The '504 patent specification does not support the Office's unbounded interpretation.

The asserted references also contradict the Office's overbroad construction of a "DNS device" and a "DNS system." As one example discussed in greater detail below, RFC 2230 describes a "domain name system" and explains that various nodes on a network may utilize this domain name system. (RFC 2230 1.) RFC 2230 describes the proxy routers R1 and R2 as nodes that interact with the domain name system by performing DNS requests that the domain name system must then process, but the routers are never described as being part of the domain name *system* itself. (*See, e.g., id.* at 2-6.) Thus, the domain name system is described as being separate and apart from the routers that merely interact with the domain name system by making DNS requests. In spite of this fact, the Office nonetheless concludes that R1 and R2 are DNS devices that are part of the claimed DNS system. (*See* Second OA at 15-18.) Thus, this reference and others, as discussed in greater detail in the sections corresponding to those references, demonstrate that the Office's construction is unreasonable and contrary to the understanding of a person of ordinary skill in the art at the time of the invention.

For these reasons and those discussed in greater detail below, the rejections are based on an improper construction of the claimed DNS system and should be withdrawn.

C. The Rejections Are Based on Incorrect Constructions of the Claimed "Indication"

Every claim of the '504 patent also recites, or incorporates by virtue of its dependency, the feature of "an indication that the domain name service system supports establishing a secure communication link." (*See* '504 patent 55:49-60:14.) The Office's construction of the recited "indication" is also incorrect and renders the Office's patentability conclusions defective for at least two reasons. First, the Office adopts a construction of the claimed indication but then concludes that the cited references disclose this feature without ever applying its construction. Second, the Office instead implicitly adopts a second, unreasonably broad construction that is disclaimed in the '504 patent specification. Thus, as discussed in greater detail below, the Office's rejections should be withdrawn.

The Office construes the recited “indication” term as “a visible message or signal to a user that the DNS system supports establishing a secure communication link.” (Second OA at 18, citing Apple Comments, Ex. A.) But the Office never applies this construction when attempting to show how the references allegedly disclose the recited indication. As one example, the Office asserts that *Solana*’s use of certificates and encryption keys discloses the recited indication, without explaining how the use of certificates and keys provides a “visible message or signal to a user.” (*See, e.g., id.* at 7, incorporating Req. at 44-45; *see also id.* at 19-25.) In fact, those skilled in the art would have understood that certificates and encryption keys were *not visible* messages or signals to a user. (Supp. Keromytis Decl. ¶ 11.) The Office similarly omits this analysis in rejections based on other references.

Although VirnetX does not agree with the Office’s purported claim construction, VirnetX’s ability to challenge the application of its construction is significantly hampered because the Office has not explained how it should be applied. As a result, Patent Owner has to guess as to the true basis for the rejection, improperly placing the burden of establishing a prima facie case of anticipation on Patent Owner rather than the Office. *In re Jung*, 637 F.3d 1356, 1362 (Fed. Cir. 2011) (“The Patent and Trademark Office (‘PTO’) satisfies its initial burden of production by ‘adequately explain[ing] the shortcomings it perceives so that the applicant is properly notified and able to respond.’” (alteration in original) (citation omitted)). By concealing the basis for its rejection in this manner, the Office has also contravened 35 U.S.C. § 132. *Chester v. Miller*, 906 F.2d 1574, 1578 (Fed. Cir. 1990) (Section 132 is violated “when a rejection is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection”).

Also, the Second Office Action applies a much broader construction of “indication” that encompasses features that neither indicate that the domain name service system supports establishing a secure communication link nor are visible to any users, such as merely returning an IP address, a public key, or a certificate demonstrating authenticity of the source of the public key. (*See, e.g.,* OA at 34, “interpreting the claimed ‘indication’ as a provision of an address is reasonably broad consistent with the specification”; *id.* at 42, “the release of the Cert RR [a certificate demonstrating authenticity of a source of a public key] by the DNS server . . . certainly indicates secure communications is supported”) This implied construction is improper because it is inconsistent with the ’504 patent specification. M.P.E.P. § 2258(I)(G) (“During reexamination, claims are given the broadest reasonable interpretation *consistent with the specification*” (emphasis added)); *see also Abbott*, 696 F.3d at 1149 (“Usually [the specification] is dispositive; it is the single best guide to the meaning of a disputed term.” (citation omitted)).

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.