Trials@uspto.gov
571.272.7822

Paper 9
Entered: October 15, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00615
Case IPR2014-00616
Case IPR2014-00618
Patent 7,921,211 B2[1]

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

SIU, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review in IPR2014-00615 and IPR2014-00618
and Denying Institution of *Inter Partes* Review in IPR2014-00616
37 C.F.R. § 42.108

---

[1] A copy of this Decision will be entered in each case. Hereinafter, using the heading style of the Scheduling Order, all papers and exhibits by the parties will be filed only in IPR2014-00615.

I. INTRODUCTION

A. Background

Microsoft Corporation ("Petitioner") filed three Petitions requesting *inter partes* review of claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60 of U.S. Patent No. 7,921,211 B2 (issued April 5, 2011) (Ex. 1001,[2] "the '211 Patent"). VirnetX Inc. ("Patent Owner") filed a Preliminary Response ("Prelim. Resp.") in each of the three proceedings, as listed in the following chart.

Case No.	**Challenged Claims**	**Petition Paper No.**	**Preliminary Response Paper No.**
IPR2014-00615	1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60	Paper 2	Paper 7
IPR2014-00616	1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60	Paper 2	Paper 7
IPR2014-00618	1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60	Paper 1	Paper 8

We have jurisdiction under 35 U.S.C. § 314. The standard for instituting *inter partes* review is set forth in 35 U.S.C. § 314(a) which provides:

> THRESHOLD.—The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311

[2] For the purposes of clarity and expediency, we use Case IPR2014-00615 as representative of the three proceedings. Unless otherwise noted, all citations to "Pet.," "Prelim. Resp.," and "Ex." refer to the Petition, Preliminary Response, and exhibits, respectively, in Case IPR2014-00615.

> and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

We determine, based on the record, that Petitioner has demonstrated, under 35 U.S.C. § 314(a), that there is a reasonable likelihood it would prevail in establishing unpatentability with respect to all of the challenged claims, claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60.

Petitioner relies on the following references:

US 6,557,037 B1	Apr. 29, 2003	(Ex. 1008, "Provino")[3]
US 6,225,993 B1	May 1, 2001	(Ex. 1009, "Lindblad")

P. Mockapetris, *Domain Names — Concepts and Facilities*, NETWORK WORKING GROUP, REQUEST FOR COMMENTS: 1034 1–55 (1987) (Ex. 1010, "RFC 1034").

E. Rescorla & A. Schiffman, *The Secure HyperText Transfer Protocol*, Enterprise Integration Technologies 1–35 (1996) (Ex. 1012, "RFC 2660").

Takahiro Kiuchi & Shigekoto Kaihara, *C-HTTP -- The Development of a Secure, Closed HTTP-based Network on the Internet*, PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, IEEE 64–75 (1996) (Ex. 1018, "Kiuchi").

Aventail Corp., *Aventail Connect v3.01/v2.51 Administrator's Guide* and *Aventail Extranet Center v3.0 Administrator's Guide* 1–194 (1996–99) (Ex. 1007, "Aventail") ('616 IPR, Ex. 1007, "Aventail").

Dave Kosiur, *Building and Managing Virtual Private Networks* (Sept. 1, 1998) ("Kosiur") ('618 IPR, Ex. 1024).

Petitioner contends that the challenged claims are unpatentable under 35 U.S.C. § 102 and/or § 103 based on the following specific grounds:

---

[3] Exhibit in the '618 IPR.

Reference(s)	Basis	Claims Challenged
Kiuchi	§ 102	1, 2, 6, 14–17, 19–23, 26–31, 33–41, 43–47, 50–55, and 57–60
Aventail	§ 102 or § 103	1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60
Provino	§ 102	1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60
RFC 1034 and one of Kiuchi, Aventail, or Provino	§ 103	20, 21, 35, 44, 45, and 59
RFC 2660 and one of Kiuchi, Aventail or Provino	§ 103	16, 27, 33, 40, 51, and 57
Lindblad and one of Kiuchi or Aventail	§ 103	32 and 56
Provino and Kosiur	§ 103	29–32 and 53–56

Petitioner also relies on two declarations provided by Dr. Roch Guerin, Exhibit 1023 in the '618 IPR and Exhibit 1021 in the '615 IPR.

B. The '211 Patent

The '211 Patent describes a system and method for establishing a secure communication link between a first computer and a second computer over a computer network. Ex. 1001, 6:36–39, 48:58–60. The user obtains a URL for a secure top-level domain name by querying a secure domain name service that contains a cross-reference database of secure domain names and corresponding secure network addresses. *Id*. at 50:27–30, 50:65–66. 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 38:61–63, 39:3–5, 51:17–21.

Claim 1 of the ’211 Patent is reproduced below:

> 1. A system for providing a domain name service for establishing a secure communication link, the system comprising:
>
> a domain name service system configured and arranged to be connected to a communication network, store a plurality of domain names and corresponding network addresses, receive a query for a network address, and indicate in response to the query whether the domain name service system supports establishing a secure communication link.

Petitioner states that the ’211 Patent is presently the subject of co-pending proceedings, as follows:

1) Civil Action No. 6:13-cv-00211-LED (E.D. Tex.), filed February 26, 2013;
2) Civil Action No. 6:12-cv-00855-LED (E.D. Tex.), filed November 6, 2012;
3) Civil Action No. 6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010;
4) Civil Action No. 6:11-cv-00018-LED (E.D. Tex), filed April 27, 2012;
5) Civil Action No. 6:13-cv-00351-LED (E.D. Tex), filed April 22, 2013 (“the 2013 litigation”);
6) Civil Action No. 6:13-mc-00037 (E.D. Tex), filed November 19, 2013; and

7) Civil Action No. 9:13-mc-80769 (E.D. Fla.), filed August 7, 2013. *See* Pet. 1.

The United States Court of Appeals for the Federal Circuit recently affirmed a jury's finding that none of claims 36, 37, 47, and 51 of the '211 Patent are invalid in an appeal of a judgment in a district court case. *See VirnetX, Inc. v. Cisco Systems, Inc.*, No. 2013-1489, 2014 WL 4548722 (Fed. Cir. Sept. 16, 2014).

C. Claim Construction

The Board interprets claim terms by applying the broadest reasonable construction in the context of the specification in which the claims reside. 37 C.F.R. § 42.100(b); *see Office Patent Trial Practice Guide*, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012).

Under the broadest reasonable standard, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). In this regard, however, we are careful not to read a particular embodiment appearing in the written description into the claim if the claim language is broader than the embodiment. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

In contrast to the broadest reasonable interpretation standard employed by the Board for an unexpired patent, the Federal Circuit employs a narrower claim construction standard when reviewing the construction of a

claim applied by the district court. *See* 37 C.F.R. § 42.100 (b) ("A claim in an unexpired patent shall be given its broadest reasonable construction in light of the specification in which it appears."); *cf. In re Rambus, Inc*., 694 F.3d 42, 46 (Fed. Cir. 2012) (Contrasting the Board's review of expired patents, which is "similar to that of a district court review," with the Board's review of unexpired patents, which involves the broadest reasonable interpretation standard).

1) Secure Communication Link

Claim 1 recites "a secure communication link." Petitioner contends that a secure communication link is a "direct communication link that provides data security through encryption." Pet. 9. Patent Owner concurs. Prelim. Resp. 17.

In *VirnetX, Inc. v. Cisco Systems, Inc.*, 2014 WL 4548722 at *4–6, 10, the Federal Circuit determined that a "secure communication link," as used in the '211 patent (and a related patent), means "a direct communication link that provides data security *and anonymity*." *Id*. at *5. Central to its claim construction, the court found, based on concessions or arguments by the parties, that the ordinary meaning of the term "security," on that record, did not apply. *See id*. at *4 ("There is no dispute that the word 'secure' does not have a plain and ordinary meaning in this context, and so must be defined by reference to the specification").

Although the parties agree that the link should be "direct," on this record, the parties do not explain how the recited link must include an implicit requirement for a "direct" link under a broadest reasonable interpretation, using either an ordinary definition, implications from the '504

Patent Specification, or other implications. Absent further input, the record does not support, and we decline to impart, such an implied requirement for purposes of this Decision. Although the Federal Circuit interpreted the "secure communication link" to be a "direct" link, *see id*. at *5, the opinion does not discuss the basis for the requirement, *see id*. at *6. In contrast to the broadest reasonable interpretation standard employed by the Board, the Federal Circuit employs a narrower claim construction standard when reviewing the construction of a claim applied by the district court.

The parties also agree that the term "secure communication link" requires encryption. Patent Owner argues that the '211 Patent specification discloses examples that include encryption, and also points to extrinsic evidence. Prelim. Resp. 17 (citing Ex. 1001, 3:10–67, 24:33–34, 33:66–67).

Notwithstanding the cited examples and extrinsic evidence, the '211 Patent Specification states that "[a] *tremendous variety* of methods have been proposed and implemented to provide security and anonymity for communications over the Internet." Ex. 1001, 1:29–31 (emphasis added). The '211 Patent Specification describes data security and anonymity as counterpart safeguards against eavesdropping that may occur while two computer terminals communicate over the Internet. *See id.* at 1:34–50. Security, in one context, may refer to protection of the data itself, to preserve the secrecy of its contents, while anonymity refers to preventing an eavesdropper from discovering the identity of a participating terminal. *See id*. at 1:36–50. Complicating the issue of what "secure" encompasses, the description of "security," according to the '211 Patent Specification generally includes "two security issues," address (anonymity) and data

security, with completely secure communications being "immune to eavesdropping." *Id*. at 1:42–46.

According to the '211 Patent Specification, "data security is *usually* tackled using some form of data encryption." Ex. 1001, 1:51–52 (emphasis added). These descriptions involving what "usually" occurs and the reference to a "tremendous variety of methods" imply that "security" may include, but does not require, encryption. In *VirnetX, Inc. v. Cisco Systems, Inc.*, 2014 WL 4548722 at *4–6, 10, the court, citing the same and similar passages in the '211 Patent and a related VirnetX patent specification, determined that "security" does not require encryption.

Further supporting the implication that security does not require encryption, the '211 Patent Specification provides a specific example that employs "unencrypted message packets," while using "different levels of authentication," and, under some circumstances, "a keyed hopping sequence." *See* Ex. 1001, col. 54, ll. 39–56. Another example shows that "unencrypted message packets" can be modified by inserting data packets into them to form a virtual private connection that "can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service." *Id*. at 1001, 54:3–7.

The '211 Patent also describes "various embodiments" which form a "secure communication" by "'hopping' different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets." *Id*. at 21:39–43. Using this hopping technique on "[p]ackets transmitted according to one or more of the inventive principles will be generally referred to as 'secure' packets or 'secure communications.'" *Id*. at 21:43–48.

The ’211 Patent also explains that “[a]ccording to the invention, a virtual private connection does not provide the same level of security . . . as a virtual private network.” *Id*. at 54:3–4. In other words, given the different examples and general descriptions that encompass a wide variety of techniques, the ’211 Patent Specification describes different levels of security by using different methods to obtain different security levels, rendering the term “secure” relative.

Therefore, similar to the determination in the Federal Circuit, on this record, neither Petitioner nor Patent Owner demonstrate persuasively that the ’211 Patent Specification requires “encryption” for a “secure communication link.” Notwithstanding the Federal Circuit’s determination on that record that a “secure communication link” requires “anonymity” (note 4), the parties do not urge anonymity as an implicit feature of the claim term in this proceeding. No apparent reason exists on this record to require anonymity as an implied limitation.

As noted, in contrast to the broadest reasonable interpretation standard employed by the Board for an unexpired patent, the Federal Circuit employs a narrower claim construction standard when reviewing the construction of a claim applied by the district court. Moreover, in a related *inter partes* proceeding between the same parties and involving a related patent of the ’211 Patent, Patent Owner argued that the “patent specification supports the view” that anonymity is not required: “[a] link that prevents others from understanding the communications sent over it may still be considered ‘secure’ even if the communicating parties do not enjoy any anonymity.” *Apple Inc. v. Virnetx Inc*., Case IPR2014-00237, slip op. at 22 (PTAB Mar. 6, 2014) (Paper 12 (citing U.S. Patent No. 8,504,697 B2, 39:40–58)).

Two technical dictionaries on this record support Patent Owner's argument that the term "secure," in the context of communications, carries an ordinary meaning that does not require anonymity. For example, "security" is "[t]he existence and enforcement of techniques which restrict access to data, and the conditions under which data may be obtained." Ex. 3002 (MCGRAW-HILL DICTIONARY OF SCIENTIFIC AND TECHNICAL TERMS 1780 (5th ed. 1994)). Similarly, a "security service" carries the following meaning:

> (1) A service, provided by a layer of communicating open systems, that ensures adequate security of the systems or of data transfers. . . . (2) The capability of the system to ensure the security of system resources or data transfers. Access controls, authentication, data confidentiality, data integrity, and nonrepudiation are traditional data communications security services.

Ex. 3003 (IEEE 100, THE AUTHORITATIVE DICTIONARY OF IEEE STANDARDS TERMS 1016 (7th ed. 2000) (emphasis omitted), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4116807).[4]

Based on the foregoing discussion, for this Decision, the term "secure communication link" mean "a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation. methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping."

[4] The Board cited this evidence in the related *inter partes* proceeding involving a common specification with the '211 Patent. *Apple Inc. v. Virnetx Inc.*, Case IPR2014-00237, slip op. at 9–10 (PTAB May 14, 2014) (Paper 15, Institution Decision).

2) Indicate/indicating

Claim 1 recites "indicate . . . whether the domain name service system supports establishing a secure communication link." Petitioner contends that "indicate" means "a visible or non-visible message or signal that the DNS system supports establishing a secure communication link, including the establishment of the secure communication link itself." Pet. 8. Patent Owner argues that "indicating" does not include establishment of the secure communication link itself. Prelim. Resp. 16.

Neither Petitioner nor Patent Owner point to an explicit definition of the term "indicate" in the Specification. The term "indication" ordinarily means "the action of indicating" or "something (as a signal, sign, suggestion) that serves to indicate." Ex. 3001 (WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1150 (1971)). The term "indicate" ordinarily means "to point out or point to or toward with more or less exactness" or "to show the probable presence or existence or nature or course of." *Id*. On this record, the Specification is not inconsistent with the ordinary meaning or Petitioner's construction. *See, e.g.*, Ex. 1001, 40:49–41:15 (sending a "host unknown" signal if a user is not authorized, but simply establishing a link if a user is authorized).

Therefore, for purposes of this Decision, the term "indication" broadly, but reasonably, means "something that shows the probable presence or existence or nature of." In accordance with this construction, in context of claim 1, an indication that a secure communication link is in operation constitutes an indication that the system supports establishing a secure communication link.

3) Other Claim Terms

The parties do not disagree materially about other claim terms involved in this proceeding. It is not necessary to define explicitly other claim terms for purposes of this Decision.

II. ANALYSIS

A. Cited References

1) Overview of Kiuchi

Kiuchi discloses a closed Hyper Text Transfer Protocol (HTTP)-based network (C-HTTP) for a closed group of institutions, in which each member is protected by its own firewall. Ex. 1018, 64, cols. 1–2. Communication is made possible with a client-side proxy (for one institution), a server-side proxy (for another institution), and a C-HTTP name server that provides both client-side and server-side proxies with each peer's public key and Nonce values for both request and response. *Id*. at 64–65.

The client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values, which are encrypted and certified using asymmetric key encryption and digital signature technology. *Id*. at 65, col. 2.

The client-side proxy then sends an encrypted request (including the client-side proxy's IP address, hostname, request Nonce value, and symmetric data exchange key for request encryption) to the server-side proxy, which then asks the C-HTTP name server if the query from the client-side proxy is legitimate. *Id*. at 65, col. 2. If the request is confirmed

to be legitimate and access is permitted, the C-HTTP name server sends the IP address and public key of the client-side proxy and both request and response Nonce values to the server-side proxy. After receiving the client-side proxy's IP address, hostname and public key, the server-side proxy generates and sends a connection ID to the client-side proxy. After the client-side proxy accepts the connection ID from the server-side proxy, the connection is established. *Id*. at 66, col. 2.

2) Overview of Provino

Provino generally describes a secure communication system between a virtual private network and an external device. The system encrypts "at least the data portion of message packets," and the requester's address. *See* '618 IPR, Ex. 1008, 5:48, 5:43–52, 6:10–28, Abstract.

Figure 1 of Provino follows:

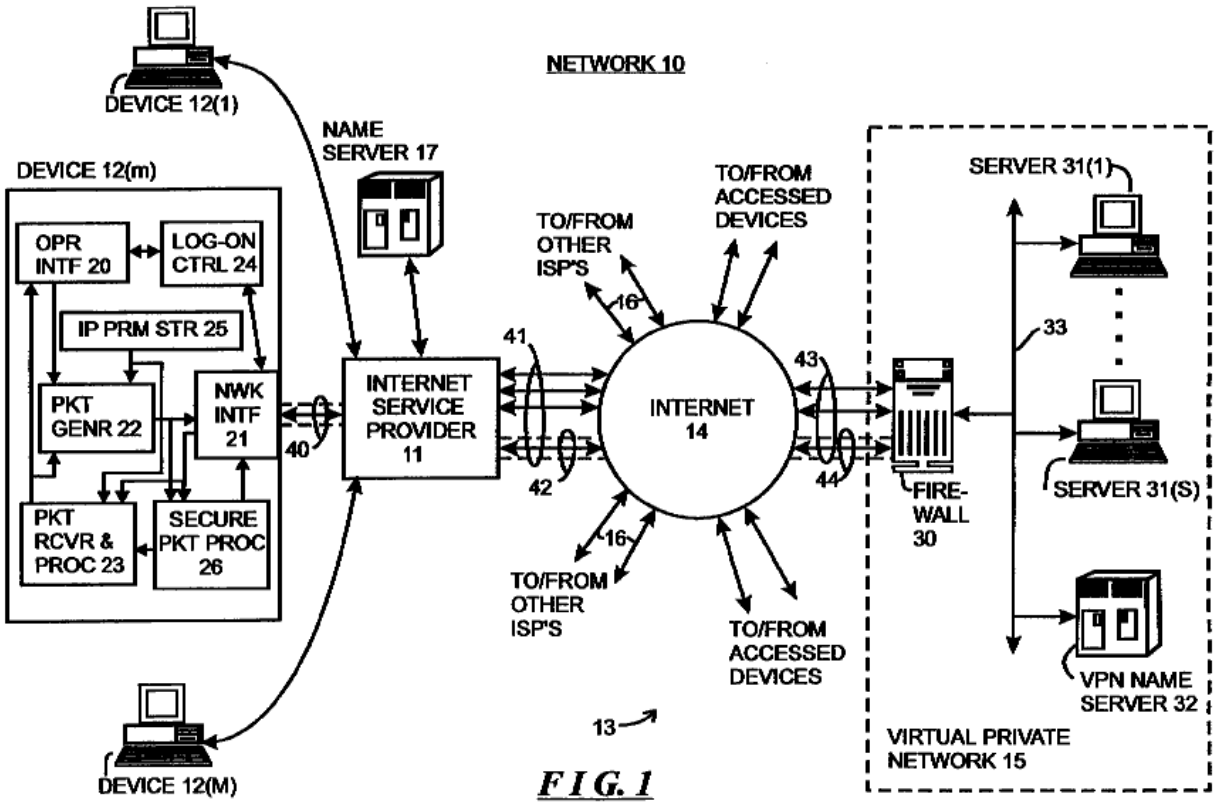

FIG. 1

Figure 1 represents Provino's system, which includes external devices 12(1)–12(m), Internet 14, and VPN 15.

According to Provino, to locate devices on a network, users typically prefer human-readable domain names, called secondary addresses, instead of integer-based addresses, all of which the Internet provides. These human-readable names (secondary addresses) must be translated, by a nameserver, into a digital integer or network address carried by a packet to indicate the destination address. Public nameservers do not have the network address for devices behind the firewall of a private network, such as VPN 15. *Id*. at 10:45–55. Nameserver 32, behind firewall 30, in VPN 15, stores the associated network address and secondary address (name) of devices in the VPN (behind the firewall). Provino's system provides a mechanism for

device 12(m) outside the firewall to use the human-readable secondary address, and obtain the integer-based network address from VPN nameserver 32, to allow external devices 12(m) to communicate with devices behind the firewall via a secure tunnel. *Id*. at 1:36–65, 3:66–4:22, 9:32–38, 10:45–67.

Provino's device 12(m) includes secure message packet processor 26 to facilitate a "secure tunnel . . . in secret by, for example, encrypting the data portion." *See id*. at 5:44–52. VPN 15 has similar devices 12(m'), including workstations, personal computers, etc. *Id*. at 6:10–28. Devices 12(m) communicate with VPN 15 and devices 13 in VPN 15. *Id*. at 5:66–6:15. During the process of obtaining the internet addresses for the human-readable addresses, firewall 30 and device 12(m) cooperate "to establish a secure tunnel therebetween, in addition to possibly providing the device 12(*m*) with . . . encryption and decryption algorithms and keys which are to be used in connection with the message packets transferred over the secure tunnel." *Id*. at 10:56–67.

In summary, Provino provides a secure tunnel through Internet 14 in a first phase to firewall 30, and in a second phase, provides the resolution between the human-readable names and encrypted Internet addresses for devices behind firewall 30 of VPN 15. *Id*. at 12:4–45. "Thereafter, . . . device 12(*m)* can use the integer Internet address to generate message packets for transfer over the Internet . . . ." *Id*. at 13:51–53; *accord id*. at 15:27–30.

Ultimately, the system provides for "easing communications . . . over a secure tunnel" between public devices on Internet 14 and private devices in VPN 15. *Id*. at 15:59–65. More specifically, in terms of Figure 1,

Provino describes a system that facilitates encrypted communications between client device 12(m) connected to ISP (internet service provider) 11 and server 31(s) located within VPN 15. *See id*. at 10:13–44; Ex. 1011 ¶¶ 28–31.

3) Overview of RFC 2660

RFC 2660 discloses a client and server authenticating each other and exchanging sensitive information confidentially using secure communication mechanisms between an HTTP client-server pair. Ex. 1012, 5:8–10, 13–14.

4) Overview of Lindblad

Lindblad discloses the use of documents with HTTP of the World Wide Web in which such documents "incorporate text, graphical images, sound, and motion video." Ex. 1009, 1:64 – 2:1. The documents may be read and displayed by a multimedia document viewer. *Id*. at 4:38–43.

5) Overview of RFC 1034

RFC 1034 discloses a name server that answers standard queries in recursive mode or non-recursive mode. Ex. 1010, 21. In non-recursive mode, the server is unable to provide an answer to the request and refers to "some other server 'closer' to the answer." In recursive mode, the server "returns either an error or the answer, but never referrals." *Id*.

6) *Overview of Kosiur*

Kosiur teaches "a wide variety of applications [that] can run on Networks," including virtual private networks. '618 IPR, Ex. 1024, 244.

For example, Kosiur teaches that a VPN can support "newer applications, such as interactive multimedia and videoconferencing," *id*. at 254, "file transfers, Web browsing, and e-mail," "IP telephony," and other "transactional traffic," *id*. at 249.

B. Preliminary Argument

Although the Petition does not exceed the page limit, Patent Owner maintains that the Petition is defective because it uses a font that "fails to comply with 37 C.F.R. § 42.6(a)(2)(ii)." *See* Prelim. Resp. 1. We decline to exercise our discretion to deny the Petition for lack of a correct font.

C. Anticipation by Kiuchi

Petitioner asserts that claims 1, 2, 6, 14–17, 19–23, 26–31, 33–41, 43–47, 50–55, and 57–60 are anticipated under 35 U.S.C. § 102 by Kiuchi. Pet. 13–50. In support of this asserted ground of unpatentability, Petitioner provides explanations as to how each claim limitation recited in claims 1, 2, 6, 14–17, 19–23, 26–31, 33–41, 43–47, 50–55, and 57–60 is disclosed by Kiuchi. Upon consideration of Petitioner's analysis and supporting evidence, and taking into account Patent Owner's Preliminary Response, we are persuaded on this record that Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to anticipation of claims 1, 2, 6, 14–17, 19–23, 26–31, 33–41, 43–47, 50–55, and 57–60 over Kiuchi.

In *VirnetX, Inc. v. Cisco Systems, Inc*., 2014 WL 4548722 at *11, the Federal Circuit held that "substantial evidence" supported a jury verdict that Kiuchi does not disclose a "direct communication." The opinion, however, does not address why the claims require a "direct" communication. As

determined above in the Claim Construction section, this record does not support, under a broadest reasonable interpretation, importing a "direct" connection or communication limitation from the '211 Patent Specification, file history, or otherwise, as an implicit limitation of the recited "secure communication link" in claim 1.

Claim 1 recites a system for providing a domain name service for establishing a secure communication link that is connected to a communication network and stores a plurality of domain names and corresponding network addresses. Claims 36 and 60 recite similar features. Petitioner argues that Kiuchi discloses "client- and server-side proxies, working in conjunction with a C-HTTP name server," that the C-HTTP name server of Kiuchi "automatically and transparently perform[s] . . . name resolution and establishment of secure connections," that the system is "configured and arranged to be (and is) connected to the Internet (a communication network)," and that the "C-HTTP name server stores . . . information . . . and uses it to resolve hostnames into IP addresses in response to queries." Pet. 23–24 (citing Ex. 1018, 64–65; §§ 2.2, 2.3(1)–(2)). Petitioner has made a sufficient showing that Kiuchi discloses a service that is connected to a communication network (e.g., an "HTTP (Hypertext Transfer Protocol)-based network (C-HTTP) which can be built on the Internet," Ex. 1018, 64) and stores a plurality of domain names and corresponding network addresses (e.g., the C-HTTP contains and "sends the IP address and public key of the server-side proxy and both request and response Nonce values," Ex. 1018, 65).

Claim 1 recites a domain name service system that receives a query for a network address and indicates in response to the query whether the

domain name service system supports establishing a secure communication link. Claims 36 and 60 recite similar features. Petitioner argues that Kiuchi discloses a "client-side proxy [that] receives a request from a user agent for a resource associated with a hostname specified in a URL," that "the C-HTTP name server receives a request for a network address," and "the C-HTTP name server returns a network address." Pet. 25–27 (citing Ex. 1018, 65–66). Petitioner contends that Kiuchi discloses receiving a query for a network address (e.g., a "client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL," Ex. 1018, 65) and indicating whether the system supports establishing a secure communication link (e.g., "[i]f the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values," Ex. 1018, 65). Patent Owner has not disputed Petitioner's contention at this time.

Petitioner identifies the user agent, the client side proxy, or both as a first location, and the server side proxy, server, or both as a second location. Pet. 34–35. Petitioner maintains, under one interpretation, that Kiuchi discloses "a C-HTTP [secure] connection between the client-side proxy and the server-side proxy, which is between the user agent and destination origin server in the closed network." *See* Pet. 9–10 (discussing the broadest reasonable construction of "between"); 34 (citing Ex. 1018, 65–66, Ex. 1021 ¶¶ 21–27); Prelim. Resp. 20–21 (arguing that "each phrase uses plain and ordinary language"). A plain and customary meaning of the term "between" supports Petitioner's alternative interpretation: "between" means "in the

space that separates."[5] Kiuchi discloses a connection that is "in the space that separates" the user and the server (i.e., "between" the client and secure server). On this record, Petitioner demonstrates a reasonable likelihood that it would prevail with respect to anticipation of claims 16, 27, 33, 40, 51, and 57.

Petitioner further explains how Kiuchi discloses each limitation of claims 2, 6, 14–17, 19–23, 26–31, 33–35, 37–41, 43–47, 50–55, and 57–59, and demonstrates a reasonable likelihood that it would prevail with respect to anticipation of these claims. Pet. 30–51. In addition, Patent Owner has not disputed Petitioner's contentions with respect to these claims at this time.

D. Anticipation by Provino

Petitioner asserts that claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60 are anticipated under 35 U.S.C. § 102 by Provino. '618 Pet. 13–50. In support of this asserted ground of unpatentability, Petitioner provides explanations as to how Provino discloses each claim limitation recited in the listed claims. *Id*. at 25–50. Upon consideration of Petitioner's analysis and supporting evidence, and taking into account Patent Owner's Preliminary Response, Petitioner demonstrates a reasonable likelihood that it would prevail with respect to anticipation of claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60 by Provino.

Claim 1 recites a system for providing a domain name service for establishing a secure communication link that is configured and arranged to

[5] WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 209 (1971) (Ex. 3003, 3).

be connected to a communication network and stores a plurality of domain names and corresponding network addresses. Claims 36 and 60 recite similar features. Petitioner explains that Provino's system provides an integer address from domain name servers (DNS) 17, 32 and provides communications over an encrypted secure tunnel. *See* '618 Pet. 13–14, 20–24, 25–29. By providing for authentication and a firewall, and by encrypting the data and the address, Provino establishes "a communication link that provides data security and anonymity." *See* '618 Ex. 1008, 10:56–65 15:21–39, 12:17–45, 16:1-8.

Claim 1 also recites a domain name service system that is "configured and arranged to . . . receive a query for a network address, and indicate . . . whether the domain name service system supports establishing a secure communication link." Claims 36 and 60 recite similar features. Petitioner explains that Provino's server 17, firewall 30, and VPN name server 32, each receive queries by client device 12(m), and that the system provides several indications by sending one or more of the following signals: a firewall address, an integer address, a server address, and encryption and decryption information. *See* '618 IPR, Pet. 28–29, 40–41 (discussing claims 36 and 41, which recite related forms of "indication" or "indicating").

On this record, Petitioner demonstrates a reasonable likelihood of prevailing in showing that Provino anticipates claim 1. Petitioner further explains how Provino discloses each limitation of claims 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60, and demonstrates a reasonable likelihood of prevailing in showing that Provino anticipates these claims. *Id*. at 29–50.

E. Obviousness over Kiuchi or Provino, and RFC 1034

Petitioner asserts that claims 20, 21, 35, 44, 45, and 59 are unpatentable under 35 U.S.C. § 103(a) over Kiuchi or Provino, and RFC 1034. Pet. 51; '618 IPR, Pet. 50–51. In support of this asserted ground of unpatentability, Petitioner provides explanations as to how the claim limitations recited in claims 20, 21, 35, 44, 45, and 59 are disclosed or suggested by the combination of Kiuchi or Provino, and RFC 1034. *See, e.g.*, Pet. 51–52.

Claim 20 recites a domain name database. Claims 21, 35, 44, 45, and 59 recite similar features to those recited in claim 20. Petitioner explains that RFC 1034, at least, discloses or suggests a domain name database, which is similar to the name servers disclosed in Kiuchi or Provino. *See, e.g.*, Pet. 51–52 (citing Ex. 1010, §§ 3.1, 4.1).

Petitioner asserts that one of ordinary skill in the art would have understood that a domain name database stores data "in a structured manner that allows for fast and efficient storing and searching of the data relative to other storage structures" such that it would have been obvious to one of ordinary skill in the art to have incorporated the domain name database of RFC 1034 (a structure known to store data in a structured manner for fast and efficient storing and searching) in the system of Kiuchi or Provino (in

which data is stored and retrieved) to "allow for a timely response to a query to resolve a domain name" (as disclosed by Kiuchi or Provino). Pet. 52; '618 IPR, Pet. 50–51.

Upon consideration of Petitioner's analysis and supporting evidence, and taking into account Patent Owner's Preliminary Response, on this record, Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to obviousness of claims 20, 21, 35, 44, 45, and 59 over Kiuchi or Provino, and RFC 1034.

F. Obviousness over Kiuchi and Lindblad

Petitioner asserts that claims 32 and 56 are unpatentable under 35 U.S.C. § 103(a) over Kiuchi and Lindblad. Pet. 52–54.

Claim 32 recites a plurality of services (capable of being supported by the secure communication link) that comprises audio, video, or a combination thereof. Claim 56 recites a similar feature. Petitioner argues that Kiuchi discloses "that the object transferred from the server-side proxy to the client-side proxy . . . may be in HTML format" and that Lindblad discloses that "a video object can be inserted into an HTML document, transported from a server to a client via standard HTTP, and displayed to the user." Pet. 53–54 (citing Ex. 1018, 66, § 2.3(8); Ex. 1009, 4:42–45).

As Petitioner maintains, Kiuchi discloses sending an "HTTP/1.0" response to a client-side proxy. Ex. 1018, 66. Lindblad discloses "Hyper Text Transfer Protocol (HTTP) of the World Wide Web" in which "documents . . . incorporate text, graphical images, sound, and motion video." Ex. 1009, 1:64 – 2:1. Similarly, Lindblad also discloses that a "[m]ultimedia document viewer . . . reads a multimedia document . . . and

displays the multimedia information[,] . . . [the] document in HTML format." *Id*. at 4:38–43. Hence, Kiuchi discloses sending an HTTP response over a secure communication link, and Lindblad discloses that documents transmitted via HTTP include multimedia documents, for example, "text, graphical images, sound, and motion video" (or audio, video, or a combination thereof).

Petitioner further argues that the combination of Kiuchi and Lindblad would have been obvious to one of ordinary skill in the art "because . . . these modifications . . . can easily and conveniently include motion video images in multimedia documents." Pet. 54. In other words, Petitioner essentially maintains that inserting known multimedia content into a similar protocol system predictably would have provided more information in a beneficial manner. On this record, Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to obviousness of claims 32 and 56 over Kiuchi and Lindblad.

G. *Obviousness over Provino and Kosiur*

As an alternative to anticipation, Petitioner asserts that claims 29–32 and 53–56 are unpatentable under 35 U.S.C. § 103(a) over Provino and Kosiur. '618 IPR, Pet. 52–55. These claims require the secure link to support additional applications or services including, for example, one or more of video conferencing, e-mail, a word processing program, and/or telephony. In arguing that claims 29–32 and 53–56 would have been obvious, Petitioner relies on Kosiur's description of a wide variety of known features for VPNs, including various protocols, videoconferencing, transactional traffic, interactive media, IP telephony, file transfers, Web

browsers, multimedia, and e-mail. *See id*. (citing Ex. 1023 ¶¶ 39–42, Ex. 1024, 9, 13, 243–244, 249, 254). Petitioner explains that such services or applications would have been obvious in Provino's similar system to increase the mobility and productivity of the employees operating devices in Provino. *See id*.

In other words, Petitioner essentially contends that employing known applications in similar systems including a VPN would have yielded predictable and obvious productivity and mobility gains. Upon consideration of Petitioner's analysis and supporting evidence, and taking into account Patent Owner's Preliminary Response, Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to obviousness of claims 29–32 and 53–56 over Provino and Kosiur.

H. Obviousness over Kiuchi or Provino, and RFC 2660

Petitioner asserts that claims 16, 27, 33, 40, 51, and 57 are unpatentable under 35 U.S.C. § 103(a) over Kiuchi or Provino, and RFC 2660. Pet. 55–58; '613 IPR, Pet. 55–57. In support of this asserted ground of unpatentability, Petitioner provides explanations as to how the claim limitations recited in claims 16, 27, 33, 40, 51, and 57 are disclosed or suggested by Kiuchi or Provino, and RFC 2660. *Id*.

Petitioner explains that, in the alternative event that "between" means that the secure link must start at a first location, for example, a client, and end at a second location, for example, a server, the combination of Kiuchi or Provino with RFC 2660 would have rendered that obvious. As Petitioner points out, RFC 2660, discloses a secure connection ("S-HTTP") that provides secure communication mechanisms between an HTTP client-server

pair. Ex. 1012 §§ 1, 1.1. Petitioner maintains using such a scheme would have been obvious in order to provide end-to-end encryption and personal-level security in Kiuchi or Provino. *See* Pet. 57–58 (citing Ex. 1012 § 1.1; Ex. 1021 ¶¶ 48, 50); '618 IPR, Pet. 57 (citing Ex. 1012 § 1.1, 1023 ¶¶ 44, 46, 47).

Upon consideration of Petitioner's analysis and supporting evidence, and taking into account Patent Owner's Preliminary Response, on this record, Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to obviousness of claims 16, 27, 33, 40, 51, and 57 over Kiuchi or Provino, and RFC2660.

I. Aventail

In the '616 IPR, Petitioner alleges additional grounds of unpatentability of claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, 50–60 based on Aventail (alone or in combination with other references). The Board's rules for AIA post-grant proceedings, including those pertaining to institution, are "construed to secure the just, speedy, and inexpensive resolution of every proceeding." 37 C.F.R. § 42.1(b). Therefore, in order to secure just, speedy, and inexpensive resolution of the proceeding, we exercise our discretion and do not institute a review based on the asserted grounds of unpatentability based, at least in part, on Aventail. *See* 37 C.F.R. § 42.108(a) ("[T]he Board may authorize the review to proceed . . . on all or some of the grounds of unpatentability asserted for each claim.").

III. CONCLUSION

We institute an *inter partes* review of claims 1, 2, 6, 14–17, 19–23, 26–31, 33–41, 43–47, 50–55, and 57–60 under 35 U.S.C. § 102 as anticipated by Kiuchi; claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60 under 35 U.S.C. § 102 as anticipated by Provino; claims 20, 21, 35, 44, 45, and 59 under 35 U.S.C. § 103(a) as unpatentable over Kiuchi or Provino, and RFC 1034; claims 16, 27, 33, 40, 51, and 57 under 35 U.S.C. § 103(a) as unpatentable over Kiuchi or Provino, and RFC 2660; claims 29–32 and 53–56 under 35 U.S.C. § 103(a) as unpatentable over Provino and Kosiur; and claims 32 and 56 under 35 U.S.C. § 103(a) as unpatentable over Kiuchi and Lindblad.

To administer the proceedings more efficiently, we exercise our authority under 35 U.S.C. § 315(d) to consolidate IPR2014-00615 and IPR2014-00618 and conduct them as one trial. We do not institute review in IPR2014-00616.

IV. ORDER

For the reasons given, it is

ORDERED that pursuant to 35 U.S.C. § 314(a), *inter partes* review of the ’211 Patent is hereby instituted commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial;

FURTHER ORDERED that the trial is limited to the following grounds: claims 1, 2, 6, 14–17, 19–23, 26–31, 33–41, 43–47, 50–55, and 57–60 under 35 U.S.C. § 102 as anticipated by Kiuchi; claims 1, 2, 6, 14–17, 19–23, 26–41, 43–47, and 50–60 under 35 U.S.C. § 102 as anticipated by

Provino; claims 20, 21, 35, 44, 45, and 59 under 35 U.S.C. § 103(a) as unpatentable over Kiuchi or Provino, and RFC 1034; claims 16, 27, 33, 40, 51, and 57 under 35 U.S.C. § 103(a) as unpatentable over Kiuchi or Provino, and RFC 2660; claims 29–32 and 53–56 under 35 U.S.C. § 103(a) as unpatentable over Provino and Kosiur; and claims 32 and 56 under 35 U.S.C. § 103(a) as unpatentable over Kiuchi and Lindblad. No other grounds are authorized;

FURTHER ORDERED that *inter partes* review is not instituted in IPR2014-00616;

FURTHER ORDERED that no ground other than those specifically instituted above is authorized for the *inter partes* review;

FURTHER ORDERED that the trial of IPR2014-00615 is consolidated with the trial of IPR2014-00618;

FURTHER ORDERED that IPR2014-00618 is terminated administratively;

FURTHER ORDERED that all further filings by the parties will be filed only in IPR2014-00615;

FURTHER ORDERED that the case caption in IPR2014-00615 shall be changed to reflect the consolidation with IPR2014-00618 in accordance with the scheduling order;

FURTHER ORDERED that a copy of this Decision be entered into the file of IPR2014-00615, IPR2014-00616, and IPR2014-00618; and

FURTHER ORDERED that any relevant previous filings in IPR2014-00618 necessary for consideration in the consolidated case should be filed in the consolidated case (IPR2014-00615) as a separate exhibit, including, for example, a copy of Provino and Kosiur.

For PETITIONER:

W. Karl Renner
Kevin E. Greene
FISH & RICHARDSON P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
axf@fr.com
IPR38868-0007IP1@fr.com

For PATENT OWNER:

Joseph E. Palys
Naveen Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
josephpalys@paulhastings.com
naveenmodi@paulhastings.com

Jason E. Stach
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
303 Peachtree St., NE, Suite 3500
Atlanta, GA 30308
jason.stach@finnegan.com