Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.

Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATION INTERNATIONAL CORPORATION,

Patent Owner

Patent No. 7,921,211

Issued: Apr. 5, 2011

Filed: Aug. 17, 2007

Inventor: Victor Larson, *et al.*

Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00185

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,921,211 UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1-.80 & 42.100-.123

TABLE OF CONTENTS

Apple Inc. ("Petitioner" or "Apple") petitions for *Inter Partes* Review ("IPR") under 35 U.S.C. §§ 311–319 and 37 C.F.R. § 42 of claims 1, 2, 5, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 ("the Challenged Claims") of U.S. Patent No. 7,921,211 ("the '211 patent"). By its accompanying Motion for Joinder, Petitioner seeks to join this petition to IPR2014-00615, a proceeding instituted on the same patent and the same prior art. This petition presents one additional ground relative to IPR2014-00615 establishing that dependent claim 5 is unpatentable. Claim 5 is highly similar to claims 23 and 47 involved in the -00615 proceeding – each claim specifies "*authenticat[ing] the query*" with claim 5 further specifying "*using a cryptographic technique*." Claim 5 is unpatentable over the same prior art that the Board has found to show the Challenged Claims unpatentable. *See* IPR2014-00615, Paper No. 9 at 18-21. It is submitted that consideration of this additional ground on a single claim will not impose a burden on the Panel given the common prior art and similarity to issues already being considered in the -00615 proceeding, as explained in the Motion for Joinder.

I. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

The real party of interest of this petition pursuant to § 42.8(b)(1) is Apple Inc. ("Apple") located at One Infinite Loop, Cupertino, CA 95014.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The ‘211 patent is the subject of a number of civil actions including: (i) Civ. Act. No. 6:13-cv-00211-LED (E.D. Tex.), filed February 26, 2013; (ii) Civ. Act. No. 6:12-cv-00855-LED (E.D. Tex.), filed November 6, 2012; (iii) Civ. Act. No. 6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010; (iv) Civ. Act. No. 6:11-cv-00018-LED (E.D. Tex), (iv) Civ. Act. No. 6:13-cv-00351-LED (E.D. Tex), filed April 22, 2013 (“the 2013 VirnetX litigation”); (v) Civ. Act. No. 6:13-mc-00037 (E.D. Tex); and (vi) Civ. Act. No. 9:13-mc-80769 (E.D. Fld).

The ‘211 patent is also the subject of two *inter partes* reexamination nos. 95/001,789 and 95/001,856. On May 23, 2014, the Office issued a Right of Appeal Notice in the ‘789 proceeding, maintaining rejections of all 60 claims in the ‘211 patent. Similarly, on May 30, 2014, the Office issued a an Action Closing Prosecution in the ‘856 proceeding maintaining rejections of claims 1-10 and 12-60 as obvious based on Kiuchi (Ex. 1018).

The ‘211 patent is the subject of two *inter partes* reviews filed by Microsoft Corporation (IPR2014-00615 & -00618), both instituted on October 15, 2014. The ‘211 patent was also the subject of petitions for *inter partes* review filed by New Bay Capital, LLC (IPR2013-00378, dismissed); Apple, Inc. (IPR2013-00397 & -00398, not instituted); RPX Corporation (IPR2014-00174 & -00175, not instituted); and Microsoft Corporation (IPR2014-00616, not instituted).

Concurrently with this petition, Petitioner is filing one other petition for *inter partes* review of the '211 patent, identified as IPR2015-00186.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Backup Lead Counsel
Jeffrey P. Kushan (Reg. No. 43,401) **jkushan@sidley.com** (202) 736-8914	Joseph A. Micallef (Reg. No. 39,772) **jmicallef@sidley.com** (202) 736-8492

D. Service Information

Service on Petitioner may be made by e-mail, or by mail or hand delivery to: Sidley Austin LLP, 1501 K Street, N.W., Washington, D.C. 20005. The fax number for lead and backup counsel is (202) 736-8711.

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

The Director is authorized to charge the fee specified by 37 CFR § 42.15(a) to Deposit Account No. 50-1597.

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies that the '211 patent is available for *inter partes* review by Petitioner. The Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified in the petition. The '211 patent was asserted against Petitioner in proceedings alleging infringement more than one year ago, but because this petition is accompanied by a motion for joinder to IPR2014-00615, the one-year period in 35 U.S.C. § 315(b) does not apply to this petition pursuant to 35 U.S.C. § 315(c). *E.g.*, *Dell Inc. v.*

Network-1 Security Solutions, Inc., IPR2013-00385, Paper 17 at 4-5; *Microsoft Corp. v. Proxyconn, Inc.*, IPR2013-00109, Paper 15 at 4-5. This petition is presented within one month of institution of trial in IPR2014-00615 (i.e., on October 15, 2014), as required by § 122(b). For the reasons detailed in the accompanying Motion for Joinder, proceedings based on the petitions should be joined to IPR2014-00615.

B. Challenge Under 37 C.F.R. § 42.104(b) and Relief Requested

Petitioner requests an IPR of the Challenged Claims on the grounds set forth below, and requests that each of the Challenged Claims be found unpatentable. The Board has already instituted trial on Grounds 1-4 below in IPR2014-00615. Petitioner presents the same Grounds in this Petition, plus one new Ground for one additional claim (Claim 5) based on the same prior art reference used to institute trial in Ground 1. A detailed explanation why Claim 5 is unpatentable is provided below in § V.E.

The ‘211 patent issued from a string of applications allegedly dating back to an original application filed on October 30, 1998. However, the effective filing date for the embodiments recited by Challenged Claims of the ‘211 patent is no earlier than February 15, 2000.

Kiuchi qualifies as prior art under 35 U.S.C. § 102(b). Specifically, Kiuchi (Ex. 1018) is a printed publication that was presented at the 1996 Symposium on

Network and Distributed Systems Security (SNDSS) on February 22 & 23, 1996, and published by IEEE in the Proceedings of SNDSS 1996. Ex. 1018.

RFC 1034 qualifies as prior art under 35 U.S.C. § 102(b). Specifically, RFC 1034 (Ex. 1010) was published in November 1987 by the Internet Engineering Task Force (IETF). Ex. 1010.

Lindblad qualifies as prior art under 35 U.S.C. § 102(e). Specifically, Lindblad (Ex. 1009) is a patent that was filed on April 22, 1996 and issued May 1, 2001. Ex. 1009. Therefore, Lindblad is a patent that issued on an application that was filed before any of the applications to which the '211 patent claims priority.

RFC 2660 qualifies as prior art under 35 U.S.C. § 102(b). Specifically, draft 01 of RFC 2660 (Ex. 1012) was published in February 1996 by the Internet Engineering Task Force (IETF). RFC 2660 was publically distributed no later than February 1996. Ex. 1012.

C. Claim Construction under 37 C.F.R. §§ 42.104(b)(3)

Petitioner proposes use of the same constructions adopted by the Board in IPR2014-00615 and -00618.

1. Domain Name (Claims 1, 2, 5, 6, 14-17, 19-23, 26-41, 43-47, and 50-60)

The Patent Owner has asserted to the PTAB that a "domain name" means "a name corresponding to a network address." *See* Ex. 1019 at 31-32; Ex. 1020 at 28-29. In view of the Patent Owner's assertion, it is reasonable, for purposes of this

proceeding in which the broadest reasonable construction standard applies, to consider the term "domain name" as encompassing "a name corresponding to a network address."

2. Domain Name Service System (Claims 1, 2, 5, 6, 14-17, 19-23, 26-41, 43-47, and 50-60)

The Patent Owner has asserted to the PTAB and in litigation that no construction of "domain name service system" was necessary. Ex. 1013 at 24-25; Ex. 1018 at 37-39; Ex. 1020 at 34-36. According to the Patent Owner, the claims themselves define the characteristics of the domain name service system. *Id*. In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "domain name service system" as encompassing any system with the characteristics described by the claims.

In general, under a broadest reasonable construction standard, a "system" can include one or more discrete computers or devices. Ex. 1021 at 15. This is consistent with the '211 patent's specification at col. 40, lines 35-48. This section describes a domain name service system that includes a modified DNS server 2602 and a gatekeeper server 2603, which is shown as being separate from the modified DNS server. Ex. 1001 at col. 40, lines 35-48 and fig. 26. Moreover, this sections states that "although element 2602 [(the modified DNS server)] is shown as combining the functions of two servers [(the DNS proxy 2610 and DNS server

2609)], the two servers can be made to operate independently." Ex. 1001 at col. 40, lines 46-48.

Also, the Examiner in the '789 and '856 reexamination proceedings concluded that the broadest reasonable construction of a system encompasses a single or multiple devices. Ex. 1016 at 17, Ex. 1017 at 23 (a "DNS **system** is reasonably interpreted as comprising a single device or multiple devices.").

Accordingly, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "domain name service system" as encompassing any system with the characteristics specified by the claims, where the system may include one or more devices or computers.

3. Indicate/Indicating (Claims 1, 2, 5, 6, 14-17, 19-23, 26-41, 43-47, and 50-60)

The Patent Owner has asserted to the PTAB that no construction of "indicate" or "indicating" is necessary. Ex. 1019 at 44-46; Ex. 1020 at 41-43. Similarly, in litigation for the '211 patent, the Patent Owner asserted no construction of "indicate" or "indicating" was necessary, and the Court also declined to construe the term. Ex. 1013 at 31; Ex. 1015 at 28. In light of this, we consider the previous reexamination proceedings. In the '789 and '856 reexamination proceedings, the Examiner found that, under the broadest reasonable construction, the term encompassed:

> the ability of the user to communicate using a secure link after boot-up." If the user attempts to establish a secure communication link using a DNS system after booting and is able to do so, then the user has been provided a broadly recited and **discernible** "indication" that the DNS in some manner supports establishing a communication link.

Ex. 1017 at 24 (emphasis original).

The Examiner also found that, under the broadest reasonable construction, the term encompassed:

> "a visible message or signal to a user that the DNS system supports establishing a secure communication link"

Ex. 1016 at 20; Ex. 1017 at 25 (emphasis original).

The Examiner further concluded that, under the broadest reasonable construction, "[n]either the specification nor the claim language provides a basis for limiting 'indicating' to a visual indicator." Ex. 1017 at 26.

The broadest reasonable construction of "indicate" or "indicating" should thus encompass 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.

4. Secure Communication Link (Claims 1, 16-17, 20-23, 26-27, 31-32, 35-36, 47, 51, and 60)

The Patent Owner has asserted to the PTAB that "secure communication link" should mean a "direct communication link that provides data security through encryption." Ex. 1018 at 40-43; Ex. 1020 at 37-40. In view of the Patent Owner's

assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "secure communication link" as encompassing a "direct communication link that provides data security through encryption."

5. Transparently (Claims 27 and 51)

The Patent Owner has asserted to the PTAB that "transparently" means that "the user need not be involved in creating the [secure communication link]/[secure link]." Ex. 1019 at 46-47; Ex. 1020 at 43-44. In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "transparently" as encompassing "the user need not be involved in creating the [secure communication link]/[secure link]."

6. Between [A] and [B] (Claims 16, 27, 33, 40, 51, and 57)

In prior litigation on the '211 patent, the Patent Owner argued against a defendant's construction that "between" should mean "extend from one endpoint to the other," and instead stated that "between" should only apply to the "public communication paths." Ex. 1014 at 11. Under the Patent Owner's contentions, a secure communication link is "between" two endpoints where encryption is used on the public communication paths between the two endpoints, regardless of whether the encryption extends completely from the first endpoint to the second

endpoint. *Id.* In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider a secure communication link "between [A] and [B]" to encompass a secure communication link on the public communication paths between the two endpoints, regardless of whether that secure communication link fully extends from the first endpoint to the second endpoint.

IV. SUMMARY OF THE '211 PATENT

Petitioner refers the Board to the Decisions to Institute Trial in IPR2014-00615 and -00618 at pages 4 to 5 and the Petitions filed in each such proceeding for a general description of the '211 patent. Paper Nos. 2 at 10-13.

V. DETAILED DESCRIPTION WHY THE CHALLENGED CLAIMS ARE UNPATENTABLE

This request shows how the primary references above, alone or in combination with other references, disclose the limitations of the Challenged Claims, thereby demonstrating the Challenged Claims of the '211 patent are unpatentable. As detailed below, this request shows a reasonable likelihood that the Requester will prevail with respect to the Challenged Claims of the '211 patent.

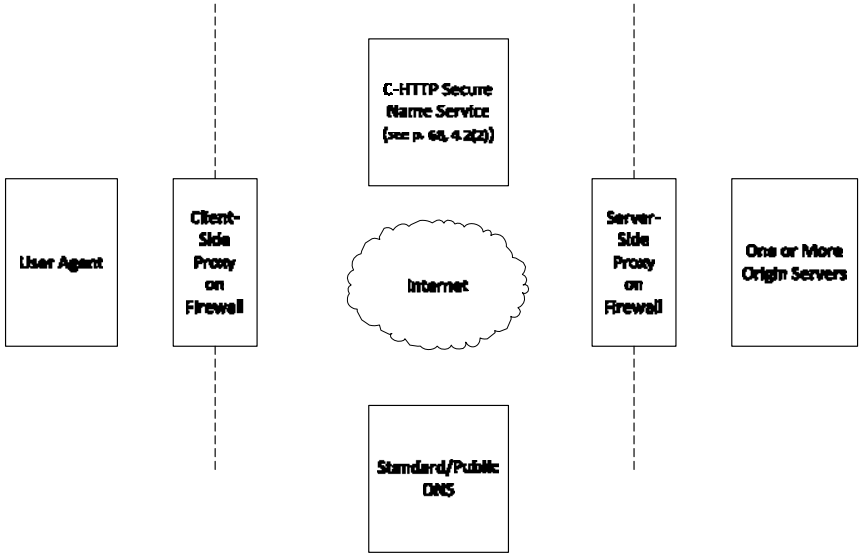
A. [GROUND 1] – Kiuchi Anticipates Claims 1, 2, 6, 14-17, 19-23, 26-31, 33-41, 43-47, 50-55, and 57-60

Kiuchi is a printed publication presented at the 1996 Symposium on Network and Distributed Systems Security (SNDSS) on February 22 & 23, 1996, and published by IEEE in the Proceedings of SNDSS 1996. *See* Ex. 1018. Kiuchi

is prior art to the '211 patent at least under § 102(b), regardless of which effective filing date in the priority chain is applied to the claims.

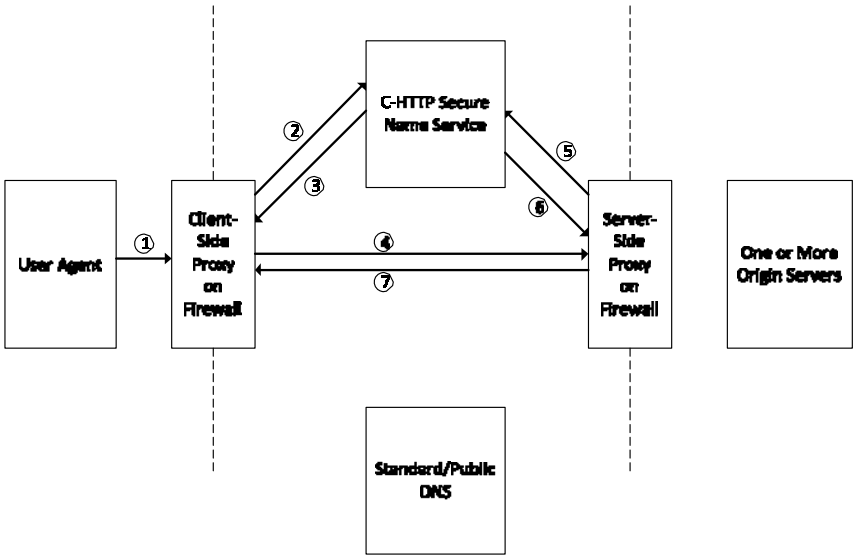
Overview of Kiuchi

Kiuchi describes a system and a protocol called "C-HTTP" that "provides secure HTTP communication mechanisms within a closed group of institutions on the Internet, where each member is protected by its own firewall." Ex. 1018 at p. 64, abstract; *see* Ex. 1021 at ¶ 16. As an example, Kiuchi describes that for "hospitals and related institutions," there is a need for "[s]ecure transfer of patient information" between hospitals, and that "medical information has to be shared among some hospitals, but it should not be made available to other sites." Ex. 1018 at p. 64, § 5; *see* Ex. 1021 at ¶ 16. Kiuchi describes that the C-HTTP protocol allows members of different institutions to communicate using "secure HTTP communication mechanisms" by way of intermediate proxies that are associated with each institution. Ex. 1018 at p. 64, Abstract; *see* Ex. 1021 at ¶ 16. The following Diagram 1 illustrates relevant parts within the C-HTTP system described by Kiuchi, and will be used to describe the C-HTTP system. *See* Ex. 1021 at ¶ 16.



(Diagram 1)

In particular, Kiuchi describes a process by which a client-side proxy, in one institution, establishes a secure C-HTTP connection with a server-side proxy, in another institution, using the C-HTTP protocol over the Internet. *See* Ex. 1018 at p. 64, § 2.1; p. 69, § 5; *see also* Ex. 1021 at ¶ 17. The C-HTTP connection uses encryption to provide a secure connection. Ex. 1018 at p. 64 §§ 2.1, 2.2; *see* Ex. 1021 at ¶ 17. Through the secure C-HTTP connection, a user agent associated with the client-side proxy may request information stored on one or more origin servers associated with the server-side proxy. *See id*. In order to establish a C-HTTP connection, Kiuchi teaches discrete steps that are described in the following block diagram. *See* Ex. 1018 at pp. 65-66, § 2.3; *see also*, Ex. 1021 at ¶ 17, Diagram 2, where each step is numbered to indicate a temporal sequence of the steps taught by Kiuchi.

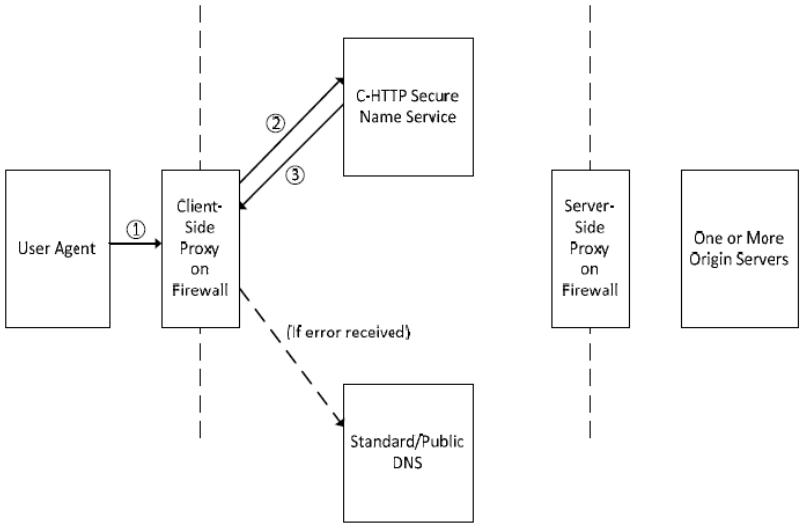


(Diagram 2)

In Kiuchi, the user agent can display HTML documents to an end-user. *See* Ex. 1018 at p. 65, § 2.3; *see also* Ex. 1021 at ¶ 18. Through interaction with the user agent, the end user may, for example, select a hyperlink URL included within an HTML document. *See id.* Kiuchi provides an example of the selected URL: "http://server.in.current.connection/sample.html=@=6zdDfldfcZLj8V!i", where "server.in.current.connection" is the hostname, "sample.html" is the name of the resource being requested, and "6zdDfldfcZLj8V!i" is a connection ID. *See* Ex. 1018 at p. 65, § 2.3*; see also* Ex. 1021 at ¶ 18.

Diagram 3 illustrates the initial steps performed by Kiuchi's system after the user selects the hyperlink (assuming that no C-HTTP connection exists). *See* Ex. 1021 at ¶ 19. These steps include: (1) a request sent from the user agent to the client-side proxy for the selected URL; (2) a request from the client-side proxy to

the C-HTTP name server for an IP address corresponding to the hostname included in the selected URL; and (3) a response from the C-HTTP name server to the client-side proxy that either includes the IP address associated with the server-side proxy or an error message. Ex. 1018 at 65-66; *see* Ex. 1021 at ¶ 19. In the last step, if the C-HTTP name server returns the IP address of the server-side proxy, then the client-side proxy begins a C-HTTP connection with the server-side proxy, and otherwise, in case of an error message, the client-side proxy performs a DNS lookup using the standard/public DNS, as illustrated by the dashed line in Diagram 3, below. *See* Ex. 1018 at p. 65, § 2.3; *see also* Ex. 1021 at ¶ 19.



(Diagram 3)

Analyzing these steps in further detail, when the end user selects the hyperlink in the displayed HTML document, the user agent sends a request for the selected URL to the client-side proxy, as illustrated by arrow (1) in Diagram 3. *See* Ex. 1018 at p. 65, § 2.3; *see also* Ex. 1021 at ¶ 20. When the client-side proxy

receives the URL (including a hostname) from the user agent, in some cases, the client-side proxy attempts to establish a new connection with the host corresponding to the hostname included in the URL. *See id.*

To establish a new connection with the host, the client-side proxy sends a request, as illustrated by arrow (2) in Diagram 3, to resolve the hostname included in the URL. *See* Ex. 1018 at p. 65, § 2.3(2); *see also* Ex. 1021 at ¶ 21. In some instances, the hostname corresponds to an origin server behind a server-side proxy and is associated with the IP address of the server-side proxy. Ex. 1018 at p. 65, § 2.3; *see* Ex. 1021 at ¶ 21. In other instances, the hostname instead corresponds to a server on the Internet outside the C-HTTP network. Ex. 1018 at p. 65, § 2.3; *see* Ex. 1021 at ¶ 21.

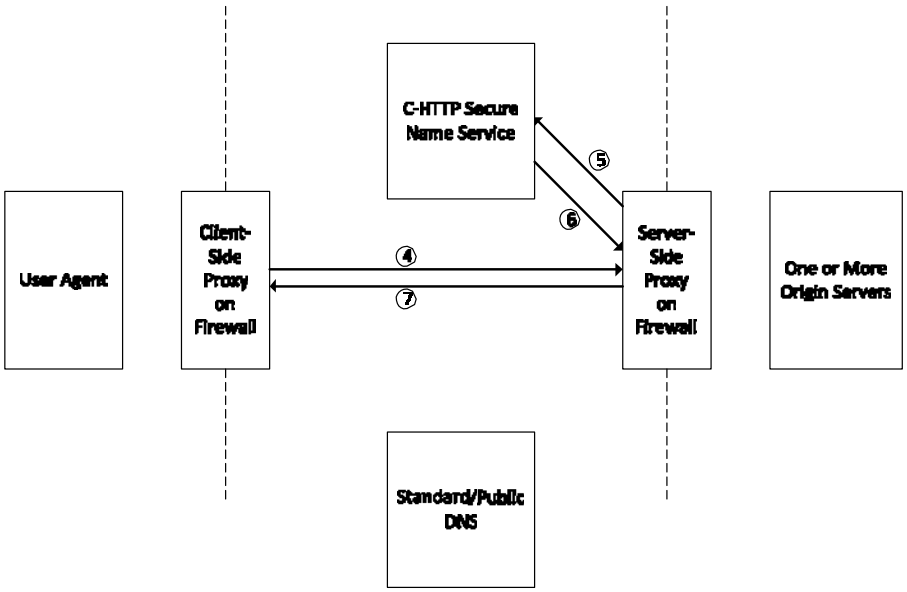
Upon receipt of the request from the client-side proxy (arrow (2)), the C-HTTP name server first authenticates the client-side proxy to determine if the request is legitimate. Ex. 1018 at p. 65, § 2.3; *see also* Ex. 1021 at ¶ 23. For example, Kiuchi describes that the communication between the client-side proxy and the C-HTTP name server is certified. *See* Ex. 1018 at p. 65; *see also* Ex. 1021 at ¶ 23. In particular, the client side proxy signs a request before sending it to the C-HTTP name server, which then verifies the signature in the request using a public key. *Id*. If successful, the C-HTTP name server authenticates the request as being legitimate. *Id*. When the request is legitimate, the C-HTTP name server

determines whether the "server-side proxy [associated with the hostname] is registered in the closed network." *Id.*

If the C-HTTP name server confirms that the server-side proxy is not registered in the closed network, or if the connection otherwise is not permitted, then the C-HTTP name server returns an error message, in response to which the client-side proxy performs a look-up with a standard/public DNS server, behaving like an ordinary HTTP proxy (as illustrated by the dashed line in Diagram 3). *See* Ex. 1018 at p. 65; *see also* Ex. 1021 at ¶ 24. The standard/public DNS server then returns to the client-side proxy an IP address of the host that corresponds to the hostname, which the client-side proxy uses to connect to the host on behalf of the user agent. *Id.*

On the other hand, if the C-HTTP name server confirms that the server-side proxy is registered in the closed network and is permitted to accept a connection from the client-side proxy, then the C-HTTP name server sends a response to the client-side proxy's request that includes "the IP address and public key of the server-side proxy and both request and response Nonce values," as illustrated by arrow (3) in Diagram 3. Ex. 1018 at p. 65, § 2.3; *see* Ex. 1021 at ¶ 25. The client-side proxy then uses the IP address, public key, and request Nonce values to contact the server-side proxy and create a C-HTTP connection with the server-side proxy. *Id.* The steps for doing so are illustrated in Diagram 4. *See* Ex. 1021 at ¶ 25.

In particular, Kiuchi describes that the client-side proxy, in response to receiving the IP address and public key of the server-side proxy, sends a "[r]equest for connection to the server-side proxy" that includes a symmetric key and other information (indicated by arrow (4) in Diagram 4). Ex. 1018 at pp. 65-66, § 2.3, steps 3-5; *see* Ex. 1021 at ¶ 26. The server-side proxy then performs a "[l]ookup of client-side proxy information" with the C-HTTP name server to determine if the client-side proxy is authorized to access the server-side proxy (arrows 5 and 6). *Id*. If the client-side proxy is authorized, then the server-side proxy sends confirmation of the C-HTTP connection to the client-side proxy (arrow 7). *Id*.



(Diagram 4)

Considering these steps in further detail, the client-side proxy, in response to receiving the IP address and associated information from the C-HTTP name server, sends a request for connection to the server-side proxy, as illustrated by arrow (4)

in Diagram 4. *See* Ex. 1018 at p. 65, § 2.3; *see also* Ex. 1021 at ¶ 27. After receiving the request, the server-side proxy "asks the C-HTTP name server whether the client-side proxy is an appropriate member of the closed network," as illustrated by arrow (5) in Diagram 4, and, in response, the C-HTTP name server "examines whether the client-side proxy is permitted to access to the server-side proxy." Ex. 1018 at pp. 65-66, § 2.3; *see* Ex. 1021 at ¶ 27. If the C-HTTP name server determines that "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, as illustrated by arrow (6) in Diagram 4. Ex. 1018 at p. 66, § 2.3; *see* Ex. 1021 at ¶ 27. The server-side proxy then responds to the client-side proxy with a message that contains a symmetric key and other information, thereby establishing the C-HTTP connection. *Id.*

Subsequently, a user agent (in the same institution as the client-side proxy) is able to securely access an origin server (in the same institution as the server-side proxy) using the C-HTTP connection. Ex. 1018 at p. 66, § 2.3; *see* Ex. 1021 at ¶ 28 As a result, members of different institutions on the Internet can communicate, via client-side and server-side proxies, using "secure HTTP communication mechanisms." Ex. 1018 at p. 64, Abstract; Ex. 1021 at ¶ 28.

Kiuchi further explains that "end-users…do not even have to be conscious of using C-HTTP based communications" and that "C-HTTP is transparent to both"

the user agent and the origin server. Ex. 1018 at p. 68, § 4.2; Ex. 1021 at ¶ 32. In particular, Kiuchi explains that, "[f]rom the view of the user agent or client-side proxy, all resources appear to be located in a server-side proxy on the firewall." Ex. 1018 at p. 66, § 2.3; Ex. 1021 at ¶ 32.

Furthermore, within each institution, Kiuchi describes that "each member is protected by its own firewall." Ex. 1018 at p. 64, abstract; *see* Ex. 1021 at ¶ 33. As an example, Kiuchi describes that "in-hospital networks are usually protected using a dual home gateway and packet filter (firewall)." Ex. 1018 at p. 67, § 4.2; Ex. 1021 at ¶ 33. In addition to the protection offered by the firewall within each institution, for further security, Kiuchi describes that "it is possible to develop C-HTTP proxies which can communicate with other secure HTTP compatible user agents and servers." Ex. 1018 at p. 69, § 4.4; Ex. 1021 at ¶ 33. Kiuchi explains that this configuration can "assure end-to-end or individual security." *Id*.

In addition, Kiuchi explains that its system uses computing devices and software, which necessarily include a machine-readable medium comprising instructions executable in a domain name service system. *See* Ex. 1021 at ¶ 34. For example, Kiuchi's client-side proxy and server-side proxy are each described as containing computer readable instructions that cause each to implement the functions performed by those items. *See* Ex. 1018 at p. 65, § 2.2; Ex. 1021 at ¶ 34. In particular Kiuchi describes that the C-HTTP proxy software is provided as

source code and provides, in the Appendices, a summary of the source code that can be used by various components of its system in implementing the functions that it provides. *See* Ex. 1018 at p. 69, § 4.4, p. 67, § 3(1), pp. 70-75; *see also* Ex. 1021 at ¶ 34. One of ordinary skill in the art would similarly understand the C-HTTP name server as containing one or more computer readable instructions that cause it to implement the functions it performs. *See* Ex. 1021 at ¶ 34.

1. Kiuchi Anticipates Claim 1

Kiuchi discloses a "*system for providing a domain name service for establishing a secure communication link*," as recited in claim 1. In particular, as described above, Kiuchi describes systems and processes for creating a closed network over the Internet that allows a user agent computer in one private network to securely access private web pages (*e.g.*, HTML documents) stored on an origin server located in a different private network. Ex. 1018 at 65; Ex. 1021 at ¶ 16. The closed network is established over the Internet by using client- and server-side proxies, working in conjunction with a C-HTTP name server, that automatically and transparently perform specialized functions, such as name resolution and establishment of secure connections. Ex. 1018 at 65; Ex. 1021 at ¶¶16-17.

Kiuchi's system includes "*a domain name service system configured and arranged to be connected to a communication network*" and "*store a plurality of domain names and corresponding network addresses*," as recited in claim 1. For

example, Kiuchi's client-side proxy, server-side proxy, C-HTTP name server, and standard DNS name server operate as a domain name service system, under the broadest reasonable interpretation of that term. Kiuchi discloses that its system is configured and arranged to be (and is) connected to the Internet (a communication network). Ex. 1018 at 64 ("In this paper, we discuss the design and implementation of a closed HTTP (Hypertext Transfer Protocol)-based network (C-HTTP) which can be **built on the Internet**." (emphasis added)); Ex. 1021 at ¶¶29-31, 34.

Further, Kiuchi's C-HTTP name server and standard DNS name server are configured to (and do) store a plurality of domain names and corresponding network addresses to resolve hostnames into IP addresses. Ex. 1018 at 65, § 2.3(1)-(2); Ex. 1021 at ¶ 29. For example, Kiuchi explains that each proxy will register an IP address and a hostname with the C-HTTP name server. Ex. 1018 at 65, § 2.2; Ex. 1021 at ¶ 29. Specifically, Kiuchi explains that when an institution wants to participate in the closed network, "it must [] install a closed-side and/or server-side proxy on its firewall [and] register an IP address . . . and a hostname" with the C-HTTP name server. Ex. 1018 at 65, § 2.2; Ex. 1021 at ¶ 29. The C-HTTP name server stores this information, and uses it to resolve hostnames into IP addresses in response to queries from authorized proxies. Ex. 1018 at 65; Ex. 1021 at ¶ 29. In this case, the hostname is a "domain name," under that terms broadest reasonable construction, because the hostname corresponds to network address.

Further, as described above, Kiuchi discloses that when the user agent requests communication with an origin server that is **not** in the closed network, then the client-side proxy accesses a standard DNS server, which a person of ordinary skill would have understood to store a plurality of domain names and corresponding network addresses to resolve hostnames into IP addresses. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶ 29. In particular, the standard/public DNS also performs domain name resolution and, in order to do so, would need to store a mapping between the IP address and domain name. *See* Ex. 1018 at p. 65, § 2.2(1); *see also* Ex. 1010 at p. 5; Ex. 1021 at ¶ 29. It was well known to one of ordinary skill in the art that the Internet is composed of multiple IP addresses and domain names. *See, e.g.*, Ex. 1010 at p. 5; Ex. 1021 at ¶ 29. Therefore the standard/public DNS server would necessarily store a plurality domain names and corresponding IP addresses to resolve hostnames into IP addresses. Ex. 1021 at ¶ 29.

Kiuchi's domain name service system is configured and arranged to "*receive a query for a network address*," as recited in claim 1. For example, the client-side proxy receives a request from a user agent for a resource associated with a hostname specified in a URL. Ex. 1018 at 65; Ex. 1021 at ¶ 20-25, 27. In response, the client-side proxy sends and the C-HTTP name server receives a request for a network address associated with the origin server in the closed network. Ex. 1018 at 65; Ex. 1021 at ¶¶ 20-23. Specifically, the client-side proxy removes the

hostname from the requested URL and then "asks the C-HTTP name server whether it can communicate with the host specified in [the] URL." Ex. 1018 at 65; Ex. 1021 at ¶¶ 20-23, 27. If the requested hostname is within the closed network and the client-side proxy is permitted access, the C-HTTP name server returns a network address (*i.e.*, an IP address). Ex. 1018 at 65; Ex. 1021 at ¶¶ 20-24, 27.

In addition, when the hostname does not correspond to an origin server in a closed network, then a standard DNS name server receives, from the client-side proxy, a request for an address associated with the origin server. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶¶ 24, 29.

Therefore, in Kiuchi, the request from the client-side proxy to the C-HTTP name server and the request from the client-side proxy to the standard DNS name server both satisfy claim 1's requirement that the domain name service system be configured "*to receive a query for a network address*" that is received by Kiuchi's domain name service system.

Kiuchi's domain name service system, under the broadest reasonable construction, is also configured and arranged to "*indicate in response to the query whether the domain name service system supports establishing a secure communication link*," as recited in claim 1. For example, Kiuchi shows the C-HTTP name server evaluates the client-side proxy's request to determine whether the hostname corresponds to a destination that is part of the closed network and

whether the connection between the user agent and the origin server is permitted. Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 23-25, 27-29. If the C-HTTP name server determines the destination is not part of the closed network, it returns an error code. Ex. 1018 at 65; Ex. 1021 at ¶¶ 19, 24. If the C-HTTP name server determines the requested hostname corresponds to a secure destination and that the connection is permitted, it will return an IP address along with other information, such as a public key and request and response Nonce values, of the server-side proxy. Ex. 1018 at 65; Ex. 1021 at ¶¶ 25-27. The return of an IP address for the server-side proxy, as opposed to an error message, is a visible or non-visible message or signal that Kiuchi's domain name service system supports establishing a C-HTTP connection between the client-side proxy and the server-side proxy. Further, the C-HTTP name server's return of the server-side proxy's public key and the request and response Nonce values to the client-side proxy are each a visible or non-visible message or signal that the system supports establishing a C-HTTP connection between the client-side proxy and the server-side proxy. Moreover, the C-HTTP name server returns this information in response to the query from the client-side proxy. 1021 at ¶¶ 25-27. Therefore, Kiuchi discloses that its domain name service system, under the broadest reasonable interpretation, indicates in response to the query whether the domain name service system supports establishing a secure communication link.

As described above, the C-HTTP connection uses encryption to provide a secure connection. Ex. 1018 at p. 64 §§ 2.1, 2.2; Ex. 1021 at ¶¶ 17, 39. Accordingly, the C-HTTP connection is a "secure communication link," under the broadest reasonable interpretation of that term, because the C-HTTP connection is a direct communication link between the client-side proxy and the server-side proxy that provides data security through encryption.

2. Kiuchi Anticipates Claim 36

Kiuchi discloses *"a non-transitory machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for*" performing the action specified in claim 36. In particular, the client-side proxy, the server-side proxy, the standard DNS server, and the C-HTTP name server described in Kiuchi each contain computer readable instructions that cause each to implement the functions performed by those items. Ex. 1018 at 65-66; Ex. 1021 at ¶ 34.

As explained in § 1, above, Kiuchi's machine-readable medium comprises instructions comprising code for "connecting the domain name service system to a communication network." For example, Kiuchi discloses that its system is configured to be (and is) connected to the Internet (a communication network). Ex. 1018 at 64; Ex. 1021 at ¶¶ 16, 17, 21.

In addition, Kiuchi's machine-readable medium comprises instructions comprising code for "storing a plurality of domain names and corresponding network addresses." As described in § 1, Kiuchi explains that each proxy will register an IP address and a hostname with the C-HTTP name server, which stores this information, and uses it to resolve hostnames into IP addresses in response to queries from authorized proxies. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶¶ 29-31. Further, as described in § 1, Kiuchi discloses that when the user agent requests communication with an origin server that is not in the closed network, then the client-side proxy accesses a standard DNS server, which a person of ordinary skill would have understood to store a plurality of domain names and corresponding network addresses to resolve hostnames into IP addresses. Ex. 1018 at 65, col. 2, ¶ 2; Ex. 1021 at ¶¶ 29-31.

In addition, Kiuchi's machine-readable medium comprises instructions comprising code for "receiving a query for a network address." As described in § 1, when the user agent requests a resource corresponding to a URL and the client-side proxy receives the request, then the C-HTTP name server receives, from the client-side proxy, a request for a network address associated with the origin server in the closed network. Ex. 1018 at 65; Ex. 1021 at ¶¶ 21-23, 27.

In addition, Kiuchi's machine-readable medium comprises instructions comprising code for "indicating in response to the query whether the domain name

service system supports establishing a secure communication link." As explained in § 1, above, Kiuchi's system includes various disclosures of indicating (according to the term's broadest reasonable construction) in response to a query whether its system supports establishing a secure C-HTTP connection, which is a secure communication link. Ex. 1018 at 65, col. 2, ¶2; 66, col. 2; Ex 1021 at ¶¶ 25, 27. For example, in response to the message request from the client-side proxy, the C-HTTP name server return of an IP address for the server-side proxy, the server-side proxy's public key, and request and response Nonce values, or an error message, all indicate, under that term's broadest reasonable construction, whether Kiuchi's DNS system supports establishing a secure communication link.

3. Kiuchi Anticipates Claim 60

Kiuchi discloses "*a method of providing a domain name service for establishing a secure communication link, the method comprising*" the steps recited in claim 60. As explained in § 1, above, Kiuchi describes various actions involved in providing a domain name service.

As explained in § 1, above, Kiuchi describes "connecting a domain name service system to a communication network" as well as "storing a plurality of domain names and corresponding network addresses" For example, as explained in § 1, above, Kiuchi's system is connected to the Internet, the C-HTTP name server and standard DNS name server store a plurality of domain names and

corresponding network addresses. Ex. 1021 at ¶¶ 16, 17, 21, 29-31. In addition, Kiuchi discloses "upon receiving a query for a network address for communication, indicating whether the domain name service system supports establishing a secure communication link." For example, as explained in § 1, above, Kiuchi's C-HTTP name server, upon receiving the query from the client-side proxy, indicates (according to the term's broadest reasonable construction), whether its system supports establishing a secure C-HTTP connection (e.g., by returning the network address, the request and response Nonce values, or the public key of the server-side proxy, or an error message).

4. Kiuchi Anticipates Claims 2 and 37

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 2 and 37. Claim 2 depends from claim 1 and specifies that "*at least one of the plurality of domain names comprises a top-level domain name*." Ex. 1001 at col. 55. Claim 37 depends from claim 36 and specifies that "*the instructions comprise code for storing the plurality of domain names and corresponding network addresses including at least one top-level domain name.*" Ex. 1001 at col. 57. Kiuchi shows an example of a domain name that may be stored at the C-HTTP name server: "University.of.Tokyo.Branch.Hospital". Ex. 1018 at p. 73, Appendix 3; Ex. 1021 at ¶ 31. In this example, one of ordinary skill in the art would understand ".Hospital" to be a top level domain, under that term's

broadest reasonable interpretation. Ex. 1021 at ¶ 31. Furthermore, as described above, Kiuchi discloses various name servers that store host names and corresponding IP addresses, and that some of those servers are standard DNS servers. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶¶ 29-31. Prior to February of 2000, one of ordinary skill in the art would understand that domain names handled by standard domain name servers would contain a top-level domain. Ex. 1021 at ¶ 31. By showing a standard nameserver connected to the Internet, Kiuchi discloses that the domain names include "a top-level domain name." Ex. 1021 at ¶ 31.

5. Kiuchi Anticipates Claim 6

As demonstrated above in §1, Kiuchi discloses "*wherein the communication network includes the Internet,*" as recited in claim 6. Ex. 1018 at 64 ("In this paper, we discuss the design and implementation of a closed HTTP (Hypertext Transfer Protocol)-based network (C-HTTP) which can be **built on the Internet**." (emphasis added)); Ex. 1021 at ¶¶ 16, 17, 21.

6. Kiuchi Anticipates Claims 14 and 38

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 14 and 38. Claims 14 and 38 depends from claim 1 and 36, respectively, and specify "*responding to the query for the network address.*" Ex. 1001 at col. 56, 57. For example, the C-HTTP name server responds to a request from the client-side proxy by either sending the IP address and public key of the

server-side proxy and both request and response Nonce values to the client-side proxy, or by sending a status code which indicates an error. Ex. 1018 at 65; Ex. 1021 at ¶¶ 19, 24-27. By sending the IP address of the server-side proxy that is associated with the host name specified in the request from the client-side proxy, as well as the other information, or an error code, the C-HTTP name server responds to a query for a network address. Ex. 1021 at ¶¶ 19, 24-27.

In addition, Kiuchi discloses that when the hostname does not correspond to an origin server in a closed network, then a standard DNS name server responds to a request from the client-side proxy by returning an IP address associated with the hostname specified in the request. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶ 24.

Therefore, under any of these examples, Kiuchi discloses that its domain name service system responds to a query for a network address. Ex. 1021 at ¶¶ 19, 24-27.

7. Kiuchi Anticipates Claims 15 and 39

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 15 and 39. Claims 15 and 39 depend from claims 1 and 36, respectively, and specify "*provid[ing] in response to the query, the network address corresponding to a domain name from the plurality of domain names and the corresponding network addresses.*" Ex. 1001 at col. 56-58. As demonstrated above, Kiuchi shows that if the C-HTTP name server determines that the request

contains a hostname corresponding to a secure destination and that a connection is permitted, the C-HTTP name server returns a response comprising an IP address corresponding to the hostname. Ex. 1018 at 65; Ex. 1021 at ¶¶ 23, 25. In addition, Kiuchi discloses that if the request contains a hostname that does not correspond to a secure destination, then a standard DNS name server responds to the request with an IP address corresponding to the hostname. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶ 24. The hostname that does not correspond to a secure destination is also a "domain name," under that terms broadest reasonable construction, because the hostname corresponds to a network address.

8. Kiuchi Anticipates Claims 16 and 40

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 16 and 40. Claim 16 depends from claim 1 and specifies the system is configured to "*receive the query initiated from a first location, the query requesting the network address associated with a domain name, wherein the domain name service system is configured to provide the network address associated with a second location, and wherein the domain name service system is configured to support establishing a secure communication link between the first location and the second location*." Ex. 1001 at col. 56. Claim 40 depends from claim 36 and specifies the machine readable medium comprising instructions for "*receiving the query for a network address associated with a domain name and*

initiated from a first location, and providing a network address associated with a second location, and establishing a secure communication link between the first location and the second location." Ex. 1001 at col. 58.

Kiuchi discloses "*receiv[ing] the query initiated from a first location, the query requesting the network address associated with a domain name*" (claim 16) and "*receiving the query for a network address associated with a domain name and initiated from a first location*" (claim 40). For example, as described above, a request is received by the C-HTTP name server from the client-side proxy. Ex. 1018 at 65; Ex. 1021 at ¶¶ 21-22. This request is a request for the IP address of the server-side proxy associated with the secure origin server that is associated with a hostname. Ex. 1018 at 65; Ex. 1021 at ¶¶ 21-23. The request is initiated by the user agent (a first location) when the user agent sends a request for content associated with a hostname to the client-side proxy. Ex. 1018 at 65; Ex. 1021 at ¶¶ 19-21. The request is also initiated by the client-side proxy (also a first location) when the client-side proxy sends the request to the C-HTTP name server. Ex. 1018 at 65; Ex. 1021 at ¶¶ 21-22. The request is a query for a network address associated with a domain name, because the request is a request for a hostname to be resolved into an IP address. Ex. 1018 at 65; Ex. 1021 at ¶¶ 21-24.

In another application of Kiuchi to claims 16 and 40, the institution in which the user agent and client-side proxy are members is a first location from which a

query for a network address is initiated. Ex. 1018 at 64, col. 2, ¶ 1; Ex. 1021 at ¶¶ 17, 22, 28, 29, 33. For example, Kiuchi discloses that the user agent is located behind a client-side proxy, which is "on the firewall of one institution" and that the origin server is located behind the server-side proxy, which is "on the firewall of another institution." Ex. 1018 at p. 64, §2.1; Ex. 1021 at ¶ 22. Therefore, Kiuchi discloses that the request for a network address sent by the client-side proxy to the C-HTTP name server is initiated from the institution in which the client-side proxy is a member. Ex. 1021 at ¶¶ 21-23.

Under any of these applications, Kiuchi discloses that its domain name service system receives a query for a network address associated with a domain name and initiated from a first location. Ex. 1021 Ex. at ¶¶ 21-27.

Kiuchi also discloses that "*the domain name service system is configured to provide the network address associated with a second location*" (claim 16) and "*providing a network address associated with a second location*" (claim 40). As described above, Kiuchi discloses that the C-HTTP name server resolves the requested hostname within the URL into an IP address, so the user agent (at one institution) can connect to the origin server (at another institution) via a connection established between the client-side proxy and the server-side proxy. Ex. 1018 at 65; Ex. 1021 at ¶¶ 17, 22, 28, 29, 33. In particular, the C-HTTP name server provides (to the client-side proxy) the IP address of the server-side proxy that is

associated with a secure origin server in a closed network at another institution. Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 25-26. Therefore, Kiuchi discloses that the C-HTTP name server provides a network address that is associated with the server-side proxy and the origin server, since the server-side proxy is a proxy for the origin server. Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 25-27. Any of the server-side proxy, the origin server, or the "another institution" are a second location.

Kiuchi also discloses "*wherein the domain name service system is configured to support establishing a secure communication link between the first location and the second location*" (claim 16) and "*establishing a secure communication link between the first location and the second location*" (claim 40). Ex. 1001 at col. 56-58. Kiuchi includes various disclosures of an established secure communication link between a first location and a second location.

For example, in one application of Kiuchi to claims 16 and 40, the "one institution" in which Kiuchi's user agent and client-side proxy are located is the first location, and the "another institution" in which Kiuchi's origin server and server-side proxy are located is the second location. In this case, the C-HTTP name server receives a request from the client-side proxy that is initiated (by a user agent) from one institution, and in response, the C-HTTP name server provides a network address (of the server-side proxy) associated with the origin server at another institution. Ex. 1018 at 65; Ex. 1021 at ¶¶ 21-23, 25. Further, Kiuchi

describes that the client-side proxy and C-HTTP name server support establishing (and the client-side proxy does establish) a C-HTTP connection between one institution (of the user agent and client-side proxy) and other institution (of the destination origin server and server-side proxy). Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 17, 22, 28, 29, 33. As described above, the C-HTTP connection is a secure communication link, under that term's broadest reasonable interpretation.

Alternatively, in another application of Kiuchi to claims 16 and 40, Kiuchi's user agent is the first location and the destination origin server is the second location. In this case, the user agent issues a request that initiates the query for an IP address sent to the C-HTTP name server by the client-side proxy, and the C-HTTP name server provides to the client-side proxy the IP address of the server-side proxy (which is associated with the origin server in a closed network). Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 21-23. The server-side proxy is associated with the destination origin server because the server-side proxy is a proxy for the origin server. Ex. 1018 at 66, col. 2; Ex. 1021 at ¶ 16, 17, 19, 21. Therefore, the server-side proxy's IP address is also associated with the destination origin server. Ex. 1021 at ¶¶ 16, 17, 19, 21. Further, when the destination origin server is in a closed network, Kiuchi describes that the client-side proxy and C-HTTP name server support establishing (and the client-side proxy does establish) a C-HTTP connection between the client-side proxy and the server-side proxy, which is

between the user agent and the destination origin server in the closed network. Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 21-27. As described above, the C-HTTP connection is server secure communication link, under that term's broadest reasonable construction.

Alternatively, in yet another application of Kiuchi to claims 16 and 40, Kiuchi's client-side proxy is the first location and the server-side proxy is the second location. In this case, the client-side proxy sends a query to the C-HTTP name server with the hostname from the requested URL, and in response the C-HTTP name server provides to the client-side proxy the IP address of the server-side proxy. Ex. 1018 at 54; Ex. 1021 at ¶¶ 21-23, 25. Further, Kiuchi describes that the client-side proxy and C-HTTP name server support establishing (and the client-side proxy does establish) a C-HTTP connection (that is, a secure communication link under that term's broadest reasonable interpretation) between the client-side proxy and the server-side proxy. Ex. 1018 at 65-66; Ex. 1021 at ¶¶ 21-27.

9. Kiuchi Anticipates Claims 17 and 41

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 17 and 41. Claim 17 depends from claim 1 and specifies the system performs the actions it was configured to perform in claim 1, with the exception that instead of requiring the domain name service system to "indicate in response to the query whether the domain name service system supports

establishing a secure communication link" as recited in claim 1, claim 17 only requires that the domain name service system "comprises an indication that the domain name service system supports establishing a secure communication link." Ex. 1001 at col. 56. As explained in §1, Kiuchi describes a system that performs each element of claim 17, because in disclosing that its C-HTTP name server indicates in response to the query from the client-side proxy whether Kiuchi's domain name service system support establishing a secure communication link, Kiuchi also discloses that its domain name service system comprises an indication that its domain name service system support establishing a secure communication link. Ex. 1021 at ¶¶ 23-27.

In addition, Kiuchi includes other disclosures that its domain name service system comprises an indication that the system supports establishing a secure communication link. For example, Kiuchi explains that if the C-HTTP name server returns an IP address, the client-side proxy will use the address to send a message to the server-side proxy. Ex. 1018 at 65; Ex. 1021 at 25-27. The server-side proxy will authenticate the message with the C-HTTP name server and if the connection is permitted, the server-side proxy will accept the connection by sending a message containing a symmetric key to the client-side proxy. Ex. 1018 at 65-66, § 2.3; Ex. 1021 at 26, 27. The message from the server-side proxy also is a visible or non-visible message or signal that the system supports establishing a C-HTTP

connection between the client-side proxy and the server-side proxy. Lastly, the establishment of the C-HTTP connection itself is a visible or non-visible message or signal the system supports establishing a C-HTTP connection between the client-side proxy and the server-side proxy.

Claim 41 depends from claim 36 and specifies that the instructions include code for "*indicating that the domain name service system supports the establishment of a secure communication link*." Ex. 1001 at 58. As explained in § 1, above, Kiuchi includes various disclosures of indicating that its domain name service system supports the establishment of a secure communication link. For example, the return of an IP address for the server-side proxy, as opposed to an error message, by the C-HTTP name server to the client-side proxy is a visible or non-visible message or signal that Kiuchi's domain name service system supports establishing a C-HTTP connection between the client-side proxy and the server-side proxy. Further, the C-HTTP name server's return of the server-side proxy's public key and the request and response Nonce values to the client-side proxy are each a visible or non-visible message or signal that the system supports establishing a C-HTTP connection between the client-side proxy and the server-side proxy. Furthermore, the message from the server-side proxy to the client-side proxy, including a symmetric key, also is a visible or non-visible message or signal

the system supports establishing (and the establishment of) a C-HTTP connection between the client-side proxy and the server-side proxy.

10. Kiuchi Anticipates Claims 19 and 43

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 19 and 43. Claims 19 and 43 depend from claims 1 and 36, respectively, and specify the system of claim 1 wherein "*the domain name service system comprises a server*" or the medium of claim 36 wherein "*the code resides on a server*." Ex. 1001 at 56-58. As explained in §1, Kiuchi teaches that the domain name service system includes a server. Ex. 1021 at ¶ 21, 27. For example, Kiuchi describes that "[a] client-side proxy asks the C-HTTP name **server** whether it can communicate with the host specified in a given URL." Ex. 1018 at 65, emphasis added; Ex. 1021 at ¶ 21, 27. Kiuchi also refers to proxies, such as the client-side proxy and server-side proxy, as "proxy **servers**." Ex. 1018 at p. 69, §4.4; Ex. 1021 at ¶ 33, 34, 37.

11. Kiuchi Anticipates Claims 20 and 44

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 20 and 44. Claims 20 depends from claim 19 and specifies "wherein the domain name service system further comprises a domain name database, and wherein the domain name database stores the plurality of domain names and the corresponding network addresses," and claim 44 depends from

claim 43 and specifies "wherein the instructions comprise code for storing a plurality of domain names and corresponding network addresses so as to define a domain name database." Ex. 1001 at cols. 56, 58. As demonstrated above in §1, Kiuchi shows that the C-HTTP name server stores a plurality of hostnames (*i.e.*, domain names) of secure destinations and corresponding IP addresses (e.g., addresses of server-side proxies in multiple institutions), and uses that information to resolve hostnames into IP addresses in response to queries from authorized proxies. Ex. 1018 at 65; Ex. 1021 at ¶ 29-31. One of ordinary skill in the art would have understood that the C-HTTP name server includes a domain name database storing the hostnames and IP addresses. Ex. 1021 at ¶ 30. Further, Kiuchi discloses that, in case of an error message being received by the client-side proxy from the C-HTTP name server, the client-side proxy performs a DNS lookup using the standard DNS, which one of ordinary skill in the art would have understood as including a domain name database storing domain names and corresponding IP addresses. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶ 30. Kiuchi therefore discloses a "domain name database" in which a plurality of domain names and corresponding network addresses are stored. Ex. 1021 at ¶ 29-31.

12. Kiuchi Anticipates Claims 21 and 45

Kiuchi discloses a system and a medium comprising instructions that anticipates claims 21 and 45. Claim 21 depends from claim 1 and specifies

"*wherein the domain name service system comprises a server, wherein the server comprises a domain name database, and wherein the domain name database stores the plurality of domain names and the corresponding network addresses.*" Ex. 1001 at col. 56. Claim 45 depends from claim 36 and specifies "wherein the code resides on a server, and the instructions comprise code for creating a domain name database configured to store the plurality of domain names and the corresponding network addresses." Ex. 1001 at col. 58. As described above in §§ 10 and 11, Kiuchi discloses various name servers (e.g., the C-HTTP name server or a standard DNS name server) that perform name resolution and include a server, which one of skill in the art would understand as including a domain name database to store a plurality of domain names and corresponding network addresses. Ex. 1018 at 65; Ex. 1021 at ¶ 29-31. Kiuchi therefore anticipates claims 21 and 45.

13. Kiuchi Anticipates Claims 22 and 46

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 22 and 46. Claims 22 and 46 depend from claims 1 and 36, respectively, and specify "*stor[ing] the corresponding network addresses for use in establishing secure communication links.*" Ex. 1001 at cols. 56, 58. For example, Kiuchi shows that the C-HTTP name server provides an IP address corresponding to a hostname to the client-side proxy. Ex. 1018 at 65; Ex. 1021 at ¶

25. In order to do so, the C-HTTP name server stores those IP addresses. Ex. 1021 at ¶ 29-31. Kiuchi further discloses that the client-side proxy uses the IP addresses to establish secure C-HTTP connections between the client-side proxy and the server-side proxy. Ex. 1018 at 65-66; Ex. 1021 at ¶ 25-27.

14. Kiuchi Anticipates Claims 23 and 47

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 23 and 47. Claims 23 and 47 depend from claims 1 and 36, respectively, and specify "*authenticat[ing] the query for the network address.*" Ex. 1001 at cols. 57, 58.

As described above, Kiuchi explains that its systems are configured to require that a client-side proxy making a request is authenticated and permitted to establish a secure communication link with a server-side proxy in a closed network. Ex. 1018 at 65, col. 2; Ex. 1021 23, 26. For example, the C-HTTP name server verifies the request from the client-side proxy for the address of the server-side proxy is legitimate and the server-side proxy is permitted to accept the connection from the client-side proxy before returning the address of the server-side proxy to the client-side proxy. Ex. 1018 at 65, col. 2; Ex. 1021 at ¶ 23, 26.

15. Kiuchi Anticipates Claims 26 and 50

Kiuchi discloses a system and a medium comprising instructions that anticipates claims 26 and 50. Claims 26 and 50 depend from claims 1 and 36,

respectively, and specify "*wherein at least one of the plurality of domain names [is configured so as to enable/enables] establishment of a secure communication link.*" Ex. 1001 at 57, 58. Kiuchi shows that certain domain names can be used to identify web servers and other secure destinations located within the C-HTTP closed network for secure communication, and can be used to establish a C-HTTP connection between the client-side proxy and the server-side proxy. Ex. 1018 at 65, col. 1, ¶ 1; Ex. 1021 at ¶ 18-23, 29. Thus, Kiuchi shows that certain domain names (*e.g.*, hostnames associated with particular origin servers or other secure destinations in a closed network) are configured to enable or do enable establishment of secure communication links. Ex. 1021 at ¶ 18-23, 29.

16. Kiuchi Anticipates Claims 27, 33, 51, and 57

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 27, 33, 51, and 57. Dependent claims 33 (from claim 1) and 57 (from claim 36) each specify the domain name service system is configured to "*enable establishment of a secure communication link between a first location and a second location"* and claims 27 (from claim 1) and 51 (from claim 36) further specify this is done "*transparently to a user at the first location*." Ex. 1001 at cols. 57, 58. Kiuchi explains that the "[e]nd-users…do not even have to be conscious of using C-HTTP based communications" and that "C-HTTP is transparent to both" the user agent and the origin server. Ex. 1018 at p. 68, § 4.2; Ex. 1021 at ¶ 32.

Therefore, Kiuchi discloses that that establishment of the C-HTTP connection is "transparent," under the broadest reasonable interpretation of that term, to a user at the user agent (a first location) because the user need not be involved in creating the secure communication link.

In another application of Kiuchi to claims 27 and 51, the institution of the user agent is a first location. In this case, as explained above, the establishment of the C-HTTP connection is transparent, under the broadest reasonable interpretation of that term, to a user at the institution because a user at the institution need not be involved in creating the secure communication link.

17. Kiuchi Anticipates Claims 28 and 52

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 28 and 52. Claims 28 and 52 depend from claims 1 and 36, respectively, and specify that "*the secure communication link uses encryption*." Ex. 1001 at cols. 57, 58. As discussed in section §1, Kiuchi teaches that the C-HTTP connection uses a "secure, encrypted protocol" for communications. Ex. 1018 at Abstract; Ex. 1021 at ¶ 16, 17, 39.

18. Kiuchi Anticipates Claims 29 and 53

Kiuchi discloses a device and a medium comprising instructions that anticipate claims 29 and 53. Claims 29 and 53 depend from claims 1 and 36, respectively, and specify that "*the secure communication link is capable of*

supporting a plurality of services." Ex. 1001 at cols. 57, 58. Kiuchi teaches this feature. For example, Kiuchi teaches that the HTTP protocol supported by the secure C-HTTP closed network is capable of supporting a variety of services: "Different application level protocols have been developed for individual network services, such as FTP, SMTP, NNTP or GOPHER [5], [6], [7], [8]. HTTP has the flexibility to be able **to provide services** similar to those which have been provided by these protocols. For example, **file transfer by FTP is accomplished by the object transfer mechanism of HTTP** and, from a functional viewpoint, the Gopher protocol can be considered a subset of HTTP. **Internet news and electronic mail services are available** with an HTTP-based graphical user interface via gateways for protocol conversions [9]. Electronic mail services within a given group of institutions can be also developed using HTTP and CGI (Common Gateway Interface) [10]." Ex. 1018 at 67, emphasis added; *see* Ex. 1021 at ¶ 35, 39. The file transfer, news, and electronic mail services described by Kiuchi are a plurality of services, under the broadest reasonable interpretation of that term, as recited in claims 29 and 53.

19. Kiuchi Anticipates Claims 30 and 54

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 30 and 54. Claims 30 and 54 depend from claims 29 and 53, respectively, and specify that "*the plurality of services comprises a plurality of*

communication protocols, a plurality of application programs, multiple sessions, or a combination thereof." Ex. 1001 at cols. 57, 58. Kiuchi teaches these features.

For example, Kiuchi describes that HTTP was chosen as the basis for the C-HTTP system because HTTP supports various user agent applications designed for different platforms and C-HTTP is transparent to those various user agents and servers. *See* Ex. 1018 at 67, § 4.1, p. 68 § 4.2; Ex. 1021 at ¶ 36. Accordingly, Kiuchi describes a plurality of application programs.

As explained above in section §18, Kiuchi teaches a plurality of services, under the broadest reasonable interpretation of that term, that may be accessed "via gateways for **protocol conversions**." Ex. 1018 at 67, emphasis added; Ex. 1021 at ¶ 34, 37, 39. Kiuchi further teaches that the services supported over the secure communication link may utilize a variety of communication protocols: "C-HTTP is not an alternative to other secure HTTP proposals, but **it can co-exist with them**. Although the current C-HTTP implementation assumes the use of HTTP/1.0 compatible user agents and servers, it is possible to develop C-HTTP proxies which can communicate with other secure HTTP compatible user agents and servers. If C-HTTP is used with **these protocols**, which assure end-to-end or individual security, both institutional and personal level security protection can be provided." Ex. 1018 at 69, § 4.4 (emphasis added).

Kiuchi further teaches that a client-side proxy is configured to process multiple different sessions with multiple different server-side proxies: "In C-HTTP, as different from ordinary HTTP, a session (virtual C-HTTP connection) is established between a client-side proxy and server-side proxy and, thus, it is not stateless. The session is finished when the client accesses another C-HTTP server or an ordinary WWW server or when the client-side or server-side proxy times out. The following ad-hoc mechanism is employed to define a session in stateless HTTP/1.0-based communication between a client-side proxy and user agent." Ex. 1018 at 65; Ex. 1021 at ¶ 39. The client-side proxy is therefore configured to transition from a first session (virtual C-HTTP connection) with a first server-side proxy to a second session (virtual C-HTTP connection) with a second server-side proxy. Ex. 1021 at ¶ 39.

20. Kiuchi Anticipates Claims 31 and 55

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 31 and 55. Claims 31 and 55 depend from claims 30 and 54, respectively, and specify that "*the plurality of application programs comprises items selected from a group consisting of the following: video conferencing, e-mail, a word processing program, and telephony*." Ex. 1001 at cols. 57, 58. Kiuchi explains that its system is built on HTTP because of its flexibility in permitting "distributed multimedia information systems with user-friendly graphical

interfaces." Ex. 1018 at 67, § 4.1, ¶ 3; Ex. 1021 at ¶ 35. Kiuchi explains that any type of data that can be transmitted via HTTP can be sent through its systems, such as electronic mail, HTML documents, and multimedia. *See* Ex. 1018 at 67; *see also* Ex. 1021 at ¶ 35. For example, Kiuchi describes that the C-HTTP supports a user agent application that provides e-mail: "Internet news and **electronic mail** services are available with an HTTP-based graphical user interface via gateways for protocol conversions. **Electronic mail** services within a given group of institutions can be also developed using HTTP and CGI (Common Gateway Interface)." Ex. 1018 at 67, § 4.1(1); Ex. 1021 at ¶ 35.

21. Kiuchi Anticipates Claims 34 and 58

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 34 and 58. Claims 34 and 58 depend from claims 33 and 57, respectively, and specify the "*query [is] initiated from the first location, wherein the second location comprises a computer, and wherein the network address is an address associated with the computer*." Ex. 1001 at cols. 57, 59. As discussed in sections §1, 8, and 15, Kiuchi includes various disclosures of these features. For example, as described above, the request that is sent from the client-side proxy to the C-HTTP name server was initiated by the user agent (a first location) when the user agent sends its request to the client-side proxy for content associated with a host-name. Ex. 1018 at 65, 66; Ex. 1021 at ¶ 18-22. This request was also initiated

by the client-side proxy itself (also a first location) when the client-side proxy sent the request. Ex. 1018 at 65; Ex. 1021 at ¶ 21-23. Also as explained above, the request from the client-side proxy to the C-HTTP name server is a query for the network address of the server-side proxy (a second location) that is part of a second institution (also a second location) and that is associated with the origin server (another example of a second location). Ex. 1018 at 65; Ex. 1021 at ¶ 21-23, 25. As another example, the institution in which the user agent and client-side proxy are members is a first location from which the request to the C-HTTP name server was initiated. Ex. 1018 at p. 64, §2.1; Ex. 1021 at ¶ 17, 22, 28, 29, 33.

In each example, a secure communication link, under the broadest reasonable interpretation of that term, is established between the first location and the second location. Furthermore, the second location comprises a computer (e.g., a computer at the origin server, the server-side proxy, or the second institution) that is associated with an address (e.g., the network address of the server-side proxy).

22. Kiuchi Anticipates Claims 35 and 59

Kiuchi discloses a system and a medium comprising instructions that anticipate claims 35 and 59. Claims 35 and 59 depend from claims 1 and 36, respectively, and specify "*wherein the domain name service system comprises a domain name database connected to a communication network and storing a plurality of domain names and corresponding network addresses for*

communication, wherein the domain name database is configured so as to provide a network address corresponding to a domain name in response to a query in order to establish a secure communication link." Ex. 1001 at cols. 57, 59.

In particular, Kiuchi discloses that the C-HTTP name server responds to a request from the client-side proxy by sending the IP address and public key of the server-side proxy, which is associated with the host name specified in the request. Ex. 1018 at 65; Ex. 1021 at ¶ 21-23, 25. Kiuchi also shows that the C-HTTP name server stores information associating hostnames (*i.e.*, domain names) of secure destinations with IP addresses, and uses that information to resolve hostnames into IP addresses in response to queries from authorized proxies. Ex. 1018 at 65, 66; Ex. 1021 at ¶ 29-31. As explained in §§ 11 and 12, above, one of ordinary skill in the art would understand that the hostnames and IP addresses that are stored at the C-HTTP name server are stored in a domain name database. Ex. 1021 at ¶ 30. In addition, as explained in §§ 8 and 15, above, Kiuchi further discloses that the C-HTTP name server provides the stored IP addresses of server-side proxies in order to establish secure C-HTTP connections between the client-side proxy and the server-side proxy. Ex. 1018 at 65; Ex. 1021 at ¶ 29-31. Therefore, Kiuchi discloses all the limitations in each of claims 35 and 59, and therefore anticipates those claims.

B. [GROUND 2] – Kiuchi In View of RFC 1034 Renders Obvious Claims 20, 21, 35, 44, 45, and 59

As explained above, Kiuchi discloses all of the limitations of claims 20, 21, 35, 44, 45, and 59. *See* §§ V.A.11, 12, 22, *above*. To the extent the Patent Owner contends Kiuchi does not show a "domain name database," this distinction does not render claims 20, 21, 35, 44, 45, and 59 patentable. In particular, RFC 1034 describes these features, and the combination of Kiuchi and RFC 1034 renders claim 20, 21, 35, 44, 45, and 59 obvious.

RFC 1034 discloses that each name server in the Domain Name System includes a domain name database for the zones managed by the name server: "Name servers are the repositories of information that make up the domain database" and the domain name database "is divided up into sections called zones, which are distributed among the name servers." Ex. 1010 at § 4.1; Ex. 1021 at 41. As a particular example, RFC 1034 describes a domain name database being shared by a name server and a resolver: "a resolver on the same machine as a name server might share a database consisting of the the [sic] zones managed by the nameserver and the cache managed by the resolver. Ex. 1010 at § 3.1; Ex. 1021 at ¶ 41.

It would have been obvious to have Kiuchi's C-HTTP name server or standard name server store the domain names and corresponding IP addresses in a domain name database as taught by RFC 1034. Ex. 1021 at ¶ 41-42. One of

ordinary skill in the art would have been motivated to make use of a domain name database as described by RFC 1034 to store the domain names and associated IP addresses, because databases store data in a structured manner that allows for fast and efficient storing and searching of the data relative to other storage structures, such as an unstructured flat text file. Ex. 1021 at ¶ 41-42. Because the number of domain names and IP addresses can be relatively large, having a fast and efficient storage would allow for a timely response to a query to resolve a domain name. Ex. 1021 at ¶ 42. It therefore would have been obvious to one of ordinary skill in the art to use the domain database of RFC 1034 in the name-servers of Kiuchi and such a combination would meet all of the elements of claims 20, 21, 35, 44, 45, and 59.

C. [GROUND 3] – Kiuchi In View of Lindblad Renders Obvious Claims 32 and 56

To the extent the Patent Owner contends Kiuchi does not show that "*the plurality of services comprises audio, video, or a combination thereof,*" this distinction does not render claims 32 and 56 patentable. In particular, Lindblad describes these features, and the combination of Kiuchi and Lindblad renders claim 32 and 56 obvious.

Lindblad describes a computer process by which "a designer of multimedia documents such as HTML pages can easily incorporate motion video titles into such HTML pages by specifying a few parameters of a desired title or a desired

portion of a title to be requested from a video server." Ex. 1009 (Lindblad) at Abstract; Ex. 1021 at ¶ 43-45. In particular, Lindblad describes:

> [A] multimedia document 206 (FIG. 2) includes an applet tag 214 which causes a multimedia document viewer 202 to execute an applet 212. Execution of applet 212 requests transmission of a bit stream of a particular title from a video server 250 and controls receipt and decoding of the bit stream by a decoder 204. Decoder 204, in response to control signals received from applet 212, decodes the received bit stream to produce a motion video image and displays the motion video image as an integral part of the representation of multimedia document 206.

Ex. 1009 at 3:25-35.

Moreover, Lindblad describes that "[i]n one embodiment, multimedia document 206 is a document in HTML format and multimedia document viewer 202 is an HTML viewer such as the Netscape World Wide Web browser." Ex. 1009 at 4:42-45; Ex. 1021 at ¶ 43-45. Thus, Lindblad describes a process by which 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 through a standard web browser. *See* Ex. 1009 at 4:42-45; Ex. 1021 at ¶ 43-45.

Kiuchi describes that the object transferred from the server-side proxy to the client-side proxy in response to a request may be in HTML format. Ex. 1018 at p.

66, § 2.3(8); *see* Ex. 1021 at ¶ 43-45. Therefore, it would have been obvious to one of ordinary skill in the art to modify the object transferred from the server-side proxy to the client-side proxy in response to include the applet described by Lindblad, and thus provide the C-HTTP system with the ability to support, for example, video and audio over the secure communication link created between the client-side proxy and the server-side proxy. *See* Ex. 1021 at ¶ 43-45. In particular, one of ordinary skill in the art would find it obvious to modify the origin server described by Kiuchi with the functionality of the video server 250 described by Lindblad, as well as include the applet described by Lindblad in a HTML page sent from the origin server. *See id.* One of ordinary skill in the art would have been motivated to modify the origin server and HTML objects described by Kiuchi in this manner, because through these modifications "a designer of a multimedia document [i.e., an HTML document] can easily and conveniently include motion video images in multimedia documents . . . thereby providing a wealth of motion video content for inclusion in multimedia documents," as described by Lindblad. Ex. 1009, 2:60 to 3:5; *see* Ex. 1021 at ¶ 43-45.

D. [GROUND 4] – Kiuchi In View of RFC 2660 Renders Obvious Claims 16, 27, 33, 40, 51, and 57

Claims 16, 27, 33, 40, 51, and 57 are anticipated by Kiuchi for the reasons set forth in §§ V.A.8 and V.A.16, above. To the extent Patent Owner contends that Kiuchi does not expressly show establishing (or establishment of) a secure

communication link between a first location and a second location – a position that would be inconsistent with its prior interpretations of the limitation – claims 16, 27, 33, 40, 51, and 57 are still unpatentable because they are obvious. In particular, were the Patent Owner to contend that a secure communication link "between" a first location and a second location must be a secure communication link that extends from the client to the secure server, rather than just an intermediate portion there-between, a person of ordinary skill in the art in February of 2000 would have considered these claims obvious based on Kiuchi in view of, *inter alia*, the information in draft 01 of RFC 2660 (Ex. 1012). Ex. 1021 at ¶ 46.

In particular, a person of ordinary skill would have considered it obvious to configure Kiuchi's user agent and origin server to implement "end-to-end secure transactions" using the Secure HTTP (S-HTTP) protocol. Ex. 1021 at ¶ 46. Kiuchi itself teaches this possibility: "[a]lthough the current C-HTTP implementation assumes the use of HTTP/1.0 compatible user agents and servers, it is possible to develop C-HTTP proxies which can communicate with other secure HTTP compatible user agents and servers." Ex. 1018 at p. 69, § 4.4; Ex. 1021 at ¶ 47. To permit this, Kiuchi describes that C-HTTP "can co-exist with" other secure HTTP proposals. *See id.* Kiuchi also describes the motivation to do so by describing the resulting benefit of assuring both institutional and personal level security: "[i]f C-HTTP is used with these protocols, which assure end-to-end or individual security,

both institutional and personal level security protection can be provided." *Id*. As an example of a secure HTTP protocol that can be used at a user agent and at an origin server, Kiuchi refers to RFC 2660 (Ex. 1012). Ex. 1018 at p. 67, § 4.2; Ex. 1021 at ¶ 47.

RFC 2660 discloses the use of encryption between clients and servers: "Secure HTTP (S-HTTP) provides secure communication mechanisms between an HTTP client-server pair in order to enable spontaneous commercial transactions for a wide range of applications." Ex. 1012 at § 1; Ex. 1021 at ¶ 48. In particular, RFC 2660 describes that ""Secure HTTP provides a variety of **security** mechanisms to **HTTP clients** and **servers**" and that "[s]everal **cryptographic** message format standards may be **incorporated** into S-HTTP **clients** and **servers**." Ex. 1012 at § 1.1; Ex. 1021 at ¶ 48. "S-HTTP provides full flexibility of cryptographic algorithms, modes and parameters." Ex. 1012 at § 1.1; Ex. 1021 at ¶ 48.

The combination of Kiuchi and RFC 2660 would result in encrypted communications between the user agent and origin server using S-HTTP messages instead of standard HTTP/1.0 messages. Ex. 1021 at ¶ 48. In this way, the use of S-HTTP could simply replace HTTP 1.0 within the C-HTTP security scheme describe by Kiuchi. Ex. 1021 at ¶ 48. As described by Kiuchi, "[t]his means that even if individual security management is not sufficient, data security can be

guaranteed. In this case, administrators of proxies on the firewall cannot know the contents of any information exchanged." Ex. 1018 at p. 69, § 4.4; Ex. 1021 at ¶ 48.

Thus, upon receipt of an S-HTTP compliant request from the user agent for information stored on an origin server, the client-side proxy would automatically establish a C-HTTP connection with the server-side proxy, as described above, and the exchange of the S-HTTP messages would ensure end-to-end encryption between the user agent and origin server. *See* Ex. 1021 at ¶ 49. If, on the other hand, the user agent is requesting information from a server that does not implement S-HTTP, the user agent would communicate using standard HTTP. *See* Ex. 1012 at § 1.1 ("S-HTTP supports interoperation among a variety of implementations, and is compatible with HTTP. S-HTTP aware clients can communicate with S-HTTP oblivious servers and vice-versa, although such transactions obviously would not use S-HTTP security features."); *see also* Ex. 1021 at ¶ 49.

Therefore, based on the motivation provided in Kiuchi, it would have been an obvious design choice to one of ordinary skill in the art to incorporate the cryptography provided by Secure HTTP, as taught by RFC 2660, into Kiuchi's user agent and origin server, in order to provide end-to-end encryption and personal-level security. Ex. 1021 at ¶ 50. Kiuchi (which discloses an encrypted/secure C-HTTP connection from the client-side proxy to the server-side

proxy) in view of RFC 2660 (which discloses encrypted/secure end-to-end communications between the user agent and origin server) discloses an encrypted/secure channel that starts at the user agent (acting as a *client*) and ends at the origin server (a *secure server*). Ex. 1021 at ¶ 50.

E. [GROUND 5] – Kiuchi Anticipates Claim 5

Kiuchi discloses a system that anticipates claim 5. Claim 5 depends from claim 2, and specifies "*wherein the domain name service system is configured to authenticate the query using a cryptographic technique*." As explained in § VA, above, and as the Board previously found, Kiuchi anticipates claim 2. *See* IPR2014-00615, Paper No. 9 at 18-23. As also explained in § VA.14 above, Kiuchi shows that the client-side proxy will send a request for a network address to the C-HTTP name server. The client-side proxy digitally signs the request, and the signature is validated by the C-HTTP name server to authenticate that the client-side proxy sent the query. Ex. 1018 at 65 ("Both the request to and response from the C-HTTP name server are encrypted and certified, using asymmetric key encryption and digital signature technology."). By validating the client-side proxy's digital signature of the request, the C-HTTP name server authenticates the request using a cryptographic technique. *See* Ex. 1021 at ¶ 23.

VII. CONCLUSION

The cited prior art references identified in this Petition establish a reasonable likelihood of success as to Petitioner's assertion that the Challenged Claims of the '211 patent are not patentable pursuant to the grounds presented in this Petition. Accordingly, Petitioner respectfully requests institution of an IPR for those claims of the '211 patent for each of the grounds presented herein.

Dated: October 31, 2014 Respectfully Submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

PETITION FOR INTER PARTES REVIEW

OF U.S. PATENT NO. 7,921,211

Attachment A:

Proof of Service of the Petition

CERTIFICATE OF SERVICE

I hereby certify that on this 31st day of October 2014, a copy of this Petition, including all attachments, appendices and exhibits, has been served in its entirety by Federal Express on the following counsel of record for patent owner:

Joseph E. Palys
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1996
E-mail: josephpalys@paulhastings.com

Naveen Modi
Paul Hastings LLP
875 15th Street NW
Washington, DC 20005
Telephone: (202) 551-1990
E-mail: naveenmodi@paulhastings.com

Jason Stach
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413

Dated: October 31, 2014

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Reg. No. 43,401
Attorney for Petitioner

PETITION FOR INTER PARTES REVIEW

OF U.S. PATENT NO. 7,921,211

Attachment B:

List of Evidence and Exhibits Relied Upon in Petition

Exhibit #	Reference Name
1001	U.S. Patent No. 7,921,211 to Larson
1002	Excerpts from the Prosecution History of the ’211 Patent
1003	[RESERVED]
1004	Curriculum Vitae of Roch Guerin
1005	[RESERVED]
1006	[RESERVED]
1007	[RESERVED]
1008	[RESERVED]
1009	U.S. Patent No. 6,225,993 to Lindblad
1010	Mockapetris, P., RFC 1034, “Domain Names – Concepts and Facilities” (November 1987)
1011	Postel, J., *et al*., RFC 1591, “Domain Name System Structure and Delegation” (March 1994)
1012	Rescorla, E., *et al*., RFC 2660, draft 10, “The Secure HyperTextTransfer Protocol” (February 1996)
1013	VirnetX’s Opening Claim Construction Brief in *VirnetX Inc. v. Cisco Sytems, Inc., et al*., 6:10-cv-417 (November 4, 2011)(EDTX)
1014	VirnetX’s Reply Claim Construction Brief in *VirnetX Inc. v.Cisco Systems, Inc., et al.*, 6:10-cv-417 (December 19, 2011)(EDTX)
1015	Memorandum Opinion and Order in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-cv-417 (April 25, 2012)(EDTX)
1016	Action Closing Prosecution (nonfinal) in *Inter Partes* Reexamination, Control No. 95/001,789 (September 26, 2012) (USPTO)
1017	Final Office Action in Inter Partes Reexamination – Right of Appeal Notice, Control No. 95/001,856 (June 25, 2013) (USPTO)
1018	Takahiro Kiuchi and Shigekoto Kaihara, “C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet,” published by IEEE in the Proceedings of SNDSS 1996
1019	Patent Owner’s Preliminary Response in IPR2013-00397

Exhibit #	Reference Name
1020	Patent Owner's Preliminary Response in IPR2013-00398
1021	Declaration of Dr. Roch Guerin re '211 Patent
1022	[RESERVED]
1023	[RESERVED]
1024	[RESERVED]
1025	[RESERVED]
1026	[RESERVED]
1027	[RESERVED]
1028	[RESERVED]
1029	[RESERVED]
1030	[RESERVED]
1031	[RESERVED]
1032	[RESERVED]
1033	[RESERVED]
1034	[RESERVED]
1035	[RESERVED]
1036	[RESERVED]
1037	[RESERVED]
1038	[RESERVED]
1039	[RESERVED]
1040	[RESERVED]

Exhibit #	Reference Name
1041	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3" (October, 1996)