UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,856	12/16/2011	7921211	43614.102	4051

22852 7590 06/25/2013

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

EXAMINER	
FOSTER, ROLAND G	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/25/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Transmittal of Communication to Third Party Requester *Inter Partes* Reexamination	Control No.	Patent Under Reexamination	
	95/001,856	7921211	
	Examiner	Art Unit	
	ROLAND FOSTER	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination prceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Right of Appeal Notice (37 CFR 1.953)	Control No.	Patent Under Reexamination
	95/001,856	7921211
	Examiner	Art Unit
	ROLAND FOSTER	3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on 02 January, 2013
Third Party(ies) on 30 January, 2013

Patent owner and/or third party requester(s) may file a notice of appeal with respect to any adverse decision with payment of the fee set forth in 37 CFR 41.20(b)(1) within **one-month or thirty-days (whichever is longer)**. See MPEP 2671. In addition, a party may file a notice of **cross** appeal and pay the 37 CFR 41.20(b)(1) fee **within fourteen days of service** of an opposing party's timely filed notice of appeal. See MPEP 2672.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

If no party timely files a notice of appeal, prosecution on the merits of this reexamination proceeding will be concluded, and the Director of the USPTO will proceed to issue and publish a certificate under 37 CFR 1.997 in accordance with this Office action.

The proposed amendment filed _____ ☐ will be entered ☐ will not be entered*

*Reasons for non-entry are given in the body of this notice.

1a. ☒ Claims 1-60 are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been cancelled.
3. ☐ Claims _____ are confirmed. [Unamended patent claims].
4. ☒ Claims 11 are patentable. [Amended or new claims].
5. ☒ Claims 1-10, 12-60 are rejected.
6. ☐ Claims _____ are objected to.
7. ☐ The drawings filed on _____ ☐ are acceptable. ☐ are not acceptable.
8. ☐ The drawing correction request filed on _____ is ☐ approved. ☐ disapproved.
9. ☐ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d) or (f). The certified copy has:
   ☐ been received. ☐ not been received. ☐ been filed in Application/Control No. _____.
10. ☐ Other _____

Attachments

1. ☐ Notice of References Cited by Examiner, PTO-892
2. ☐ Information Disclosure Citation, PTO/SB/08
3. ☐ _____

1. Introduction

This Office action addresses claims 1-60 of United States Patent No. 7,921,211 B2 (the "Larson" patent), for which reexamination was granted in the Order Granting *Inter Partes* Reexamination (hereafter the "Order"), mailed March 5, 2012, in response to a Request for Inter Partes Reexamination, filed December 16, 2011 (the "Request").

An Action Closing Prosecution ("ACP") mailed October 1, 2012 rejected original claims 1-10 and 12-16 of the Larson patent. Original claim 11 was found patentable.

The patent owner responded by filing arguments and associated evidence on January 2, 2013 (the "Response").

The third party requester responded by filing Comments on the Patent Owner's Response on January 30, 2013 (the "Comments").

Evidence Submitted After the ACP

The patent owner submitted the Supplemental Declaration of Angelos D. Keromytis, Ph.D. on January 2, 2013 (the "Supplemental Declaration"), which was after the mailing date of said ACP. Evidence submitted after an action closing prosecution (§ 1.949) in an *inter partes* reexamination filed under § 1.913 but before or on the same date of filing an appeal (§ 41.31 or § 41.61 of this title), may be admitted upon a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. 37 CFR § 1.116(e). The patent owner did not set forth a showing why the Supplemental Declaration was necessary and

was not earlier presented. After an ACP in an *inter partes* reexamination, the patent owner may once file comments limited to the issues raised in the Office action closing prosecution. 37 CFR § 1.951(a). Thus, the patent owner may not file additional comments showing why the Supplemental Declaration should be entered. The Supplemental Declaration is not of record in this proceeding. The examiner however has briefly reviewed the Supplemental Declaration, but it does not persuade the examiner to withdraw any rejection.

Conclusion

The examiner has fully considered the arguments and evidence of record provided in both the patent owner's Response and in the third party requester's Comments. Based on consideration of the entire record, the third party requester's arguments and evidence are deemed more persuasive. *See* the "Response to Arguments" section for further explanation. All prior rejections are maintained. Accordingly, this Office action is made a Right of Appeal Notice, which is a final Office action. See MPEP § 2673.01, .02. *See also* the "conclusion" section to this Office action.

Submissions after the Action Closing Prosecution (ACP)

Said Response, Comments and Supplemental Declaration were submitted after the ACP. The Supplemental Declaration is not entered for the reasons discussed above. The Response and Comments have been entered.

2. Final Decisions

2.A. Final Decisions Regarding Patentability – Right of Appeal

37 CFR § 1.953 states regarding the Examiner's Right of Appeal Notice in an *inter partes* reexamination:

> (c) The Right of Appeal Notice shall be a final action, which comprises a final rejection setting forth each ground of rejection and /or final decision favorable to patentability including each determination not to make a proposed rejection, an identification of the status of each claim, and the reasons for decisions favorable to patentability and /or the grounds of rejection for each claim....

35 U.S.C. 315, in turn, states regarding an appeal from an *inter partes* reexamination:

> (a) PATENT OWNER. — The patent owner involved in an inter partes reexamination proceeding under this chapter —
>
> (1) may appeal under the provisions of section 134...with respect to any decision adverse to the patentability of any original or proposed amended or new claim of the patent; and
>
> (2) may be a party to any appeal taken by a third-party requester under subsection (b).
>
> (b) THIRD-PARTY REQUESTER. — A third-party requester —
>
> (1) may appeal under the provisions of section 134...with respect to any final decision favorable to the patentability of any original or proposed amended or new claim of the patent....

2.B. Final Decision Favorable to Patentability (Determinations NOT to Adopt the Proposed Rejections)

Claim 11 was found patentable over the applied, prior art of record for the reasons set forth in Section 4.

2C. Final Decision Unfavorable to Patentability (Determinations to Adopt the Proposed Rejections)

A total of four principal references, in certain combinations, have been asserted in the Request as providing teachings relevant to the claims of the Larson patent.

Rolf Lendenmann, *Understanding OSF DCE 1.1 for AIX and OS/2, IBM International Technical Support Organization* (Oct. 1995) ("**Lendenmann**"), attached as Exhibit D-1 (parts 1 and 2) to the Request.

U.S. Patent No. 6,119,234 ("**Aziz**"), attached as Exhibit D-2 to the Request.

Takahiro Kiuchi and 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, 1996 ("**Kiuchi**"), attached as Exhibit D-16 to the Request.

Bryan Pfaffenberger, Netscape Navigator 3.0: Surfing the Web and Exploring the Internet, Academic Press (1996) ("**Pfaffenberger**"), attached as Exhibit D-17 to the Request.

The request also asserts additional references to explain features in the principal references or as secondary teaching references.

Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Protocol Specification Request for Comments 793 (Sept. 1981) ("**RFC 793**"), attached as Exhibit D-3.

D. Eastlake and C. Kaufman, Network Working Group, Information Sciences Institute, "Domain Name System Security Extensions," Request for Comments 2065 (Jan. 1997) ("**RFC 2065**"), attached as Exhibit D-4.

U.S. Patent No. 5,898,830 ("**Wesinger**"), attached as Exhibit D-5 to the Request.

U.S. Patent No. 5,689,641 ("**Ludwig**"), attached as Exhibit D-6 to the Request.

David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb. 21, 1998) ("**Martin**"), attached as Exhibit D-7.

Bruce Schneier, Applied Cryptography (1996) ("Schneier"), attached as Exhibit D-8.

Lawton, George, "New top-level domains promise descriptive names," Sunworld Online, September 1996 ("**Lawton**"), attached as Exhibit D-9.

Gaspoz, Jean-Paul, "VPN on DCE: From Reference Configuration to Implementation," Bringing Telecommunication Services to the People – IS&N '95, Third International Conference on Intelligence in Broadband Services and Networks, October 1995 Proceedings ("**Gaspoz**"), attached as Exhibit D-10.

U.S. Patent No. 6,269,099 ("**Borella**"), attached as Exhibit D-11 to the Request.

U.S. Patent No. 6,560,634 ("**Broadhurst**"), attached as Exhibit D-12 to the Request.

Mark Pallen, "The World Wide Web," British Medical Journal, vol. 311 at 1554 (Dec. 9, 1995) ("**Pallen**"), attached as Exhibit D-13.

R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126 (Feb. 1978) ("**Rivest**"), attached as Exhibit D-14.

U.S. Patent No. 4,952,930 ("**Franaszek**"), attached as Exhibit D-15 to the Request.

Frederic Gittler et al., "The DCE Security Service," Hewlett-Packard Journal, pp. 41-48, (Dec. 1995) ("**Gittler**"), attached as Exhibit D-18 .

2.D. Summary Regarding Those Proposed Rejections Adopted and Not Adopted by the Examiner

As will be explained in Section 3 (Response to Arguments), the rejections identified in Issues 1, 3-5, 7, 8, 11-13, 15, 17, 18, 20 and 21 (Request, pp. 31-34) remain adopted. The rejections identified in Issues 9 and 16 remain adopted except for the rejections of claims 5, 23, 27 and 50 (Issue 9) and 10-13 (Issue 16), which are withdrawn. All rejections identified in Issues 2, 6, 10, 14 and 19 are withdrawn. Claims 1-10 and 12-60 however remain rejected under at least one grounds of rejection.

2.E. Entitlement to the Benefit of an Earlier Filing Date

Requestor asserts that the instant claims are not entitled to the earliest filing date of October 30, 1998, the filing date of the oldest parent, provisional application. None of the principal references asserted by the third party requester appear to be intervening references nor does the statutory basis of rejections based upon the principal reference appear to be affected by the entitlement question. Nonetheless, the examiner agrees with the third party requester. Each of the independent claims recite a "domain name service" and a "domain name service system" limitation. A continuation-in-part application ("CIP") 09/558,210, filed April 26, 2000, includes a section entitled "Continuation-in-Part Improvements" on page 56 specifically discussing secure domain name service queries on pages 81-88. The parent applications prior to this date do not appear to even be directed to services similar to domain name lookup. Thus, the applications filed prior to April 26, 2000 fail to provide written description support nor enable the subject matter recited in claims 1-60 of the Larson patent. Accordingly, the effective filing date for claims 1-60 is no earlier than the April 26, 2000 filing date of CIP application 09/558,210.

2.F. Rejections Based upon Lendenmann (Issues 1, 3-5, 7 and 8)

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(Issue 1) Claims 1-3, 5, 6, 14-30, 33-54, and 57-60 are rejected under 35 U.S.C. 102(b) as being anticipated by Lendenmann.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

(Issue 3) Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lendenmann as applied to the respective, parent claims above, and further in view of Wesinger.

(Issue 4) Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lendenmann as applied to the respective, parent claims above, and further in view of Gaspoz.

(Issue 5) Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lendenmann in view of Gaspoz, as applied to the respective, parent claims above, and further in view of Schneier.

(Issue 7) Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lendenmann in view of Gaspoz, as applied to the respective, parent claims above, and further in view of RFC 793.

(Issue 8) Claims 31, 32, 55 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lendenmann in view of Ludwig, as applied to the respective, parent claims above, and further in view of RFC 793.

Summary

Independent claim 1 is representative of all independent claims. Independent claim 1 recites:

> **1. A system for providing a domain name service for establishing a secure communication link, the system comprising:**
>
> **a domain name service system configured to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to comprise an indication that the domain name service system supports establishing a secure communication link.**

Regarding the specification of the Larson patent for which reexamination is requested, Fig. 25 (reproduced below) is labeled "prior art."

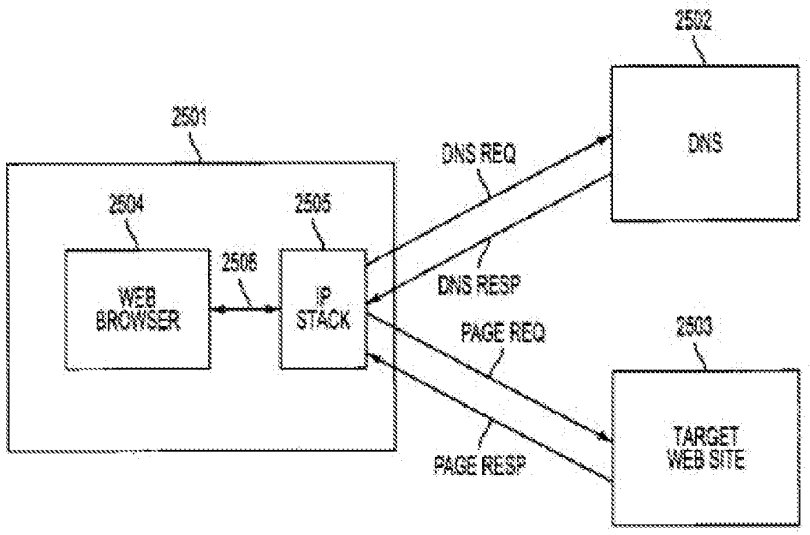


FIG. 25
(PRIOR ART)

Fig. 25 (prior art) discloses: (1) a domain name service system configured to be connected to a communication network, (2) storing a plurality of domain names and corresponding network addresses, and (3) receiving a query for a network address. Thus, all limitations in claim 1 are admitted prior art except the final limitation "to comprise an indication that the domain name service system supports establishing a secure communication link."

Nonetheless Lendenmann teaches all the limitations in representative claim 1. Lendenmann describes a Distributed Computing Environment ("DCE") providing a directory service specifically including a Cell Directory Service (CDS). (P. 10, section 1.4.4 DCE Directory Service).

Regarding the limitation "domain name service configured for connection to a communication network," Lendenmann teaches that the CDS (domain name service) is connected to a communication network, as illustrated in Fig. 15, which is reproduced below:

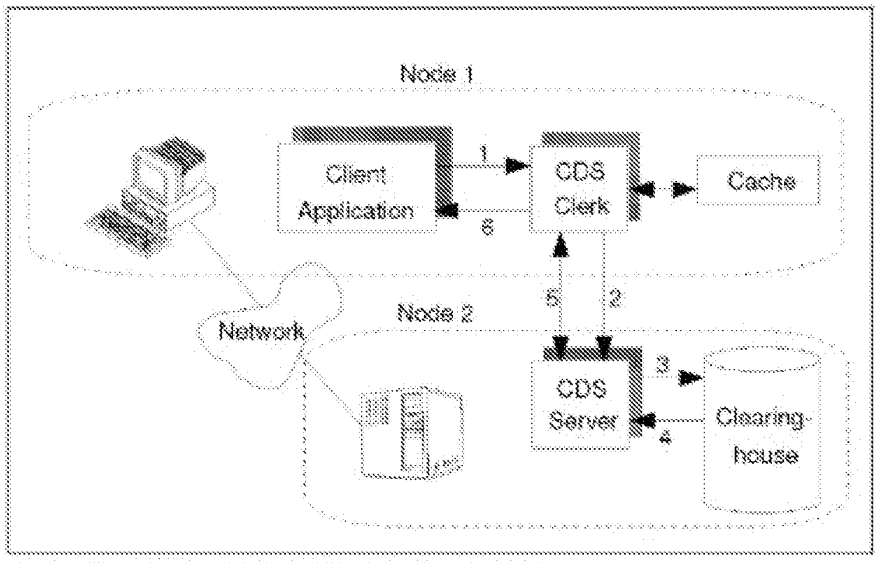


Figure 15. CDS Components Performing a CDS Look-up

Regarding the limitation "to store a plurality of domain names and corresponding network addresses" then "to receive a query for a network address," Lendenmann teaches regarding the CDS (domain name service) at p. 21, section 2.2:

> The directory service component that controls names inside a cell is called the Cell Directory Service (CDS). The CDS stores names of resources in that cell so that when given a name, CDS returns the network address of the named resource.

See also the CDS lookup process described on pages 29-34.

Regarding the limitation to provide an "indication that the domain name service supports establishing a secure communications link," a query from a client to a directory service (CDS) server via a network is made by a remote procedure call, as illustrated in Fig. 15, which is reproduced below. *See also* pp. 9 and 173.

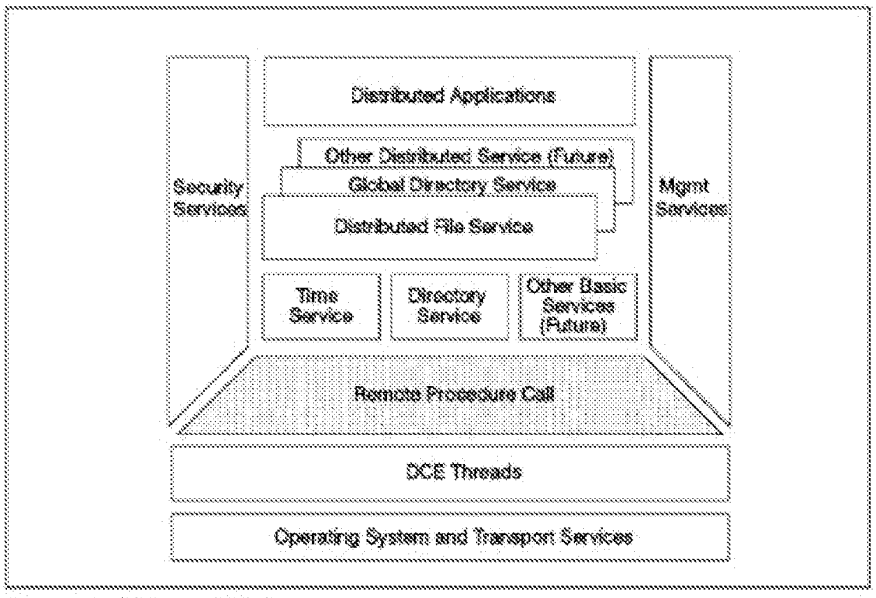


Figure 62. RPC as a DCE Component

Lendenmann further teaches that RCP calls relies upon well-known authentication algorithms, such as shared-secret key and public key (p. 192, section 10.4.1) including supplying the requesting client with a session key and a service ticket encrypted with server's session key (i.e., digitally signed certificate) (p. 194). The client encrypts the RPC call with the session key, which the "server immediately challenges...by sending it a randomly generated number which the client has to encrypt with the session key and return to the server." P. 194, section 10.4.4. The client transmits the encrypted response, which the server decrypts using the server's session

key obtained from the decrypted service ticket. If the decrypted random number matches, then the "session key is used in further communication over the binding." *Id.* Thus, the sending of the "randomly generated number" is an indication that the domain name service (CDS reached via a RCP call via the network) supports the establishment of subsequent, secure communication link using a shared secret key (the session key) for encryption/decryption.

By returning the network address corresponding to a secure domain name, the Cell Directory Service (CDS) also provides "an indication...." as recited in the claim. Request, Exhibit F-1 (Claim Chart), p. 13. Similarly, by only performing operations for users authorized using access control lists (ACLs), the CDS provides an indication that supports establishing a secure communication link. (*Id.* at 14).

Incorporation by Reference

Thus, the third party requester proposed rejection of claims identified above as set forth on pages 11-17, 31, 32 and Exhibit F-1 (claim chart), are adopted and incorporated by reference.

2.G. Rejections Based upon Aziz (Issues 9, 11-13, 15)

Claim Rejections - 35 USC § 102

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

(Issue 9) Claims 1, 2, 6-9, 14-22, 24, 25, 28, 33-49, 51, 52 and 57-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Aziz.

Claim Rejections - 35 USC § 103

(Issue 11) Claim 3, 4, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz as applied to the respective, parent claims above, and further in view of Lawton.

(Issue 12) Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz as applied to the respective, parent claims above, and further in view of Franaszek.

(Issue 13) Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz as applied to the respective, parent claims above, and further in view of Schneier.

(Issue 15) Claims 29-32 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz, as applied to the respective, parent claims above, and further in view of Ludwig.

Summary

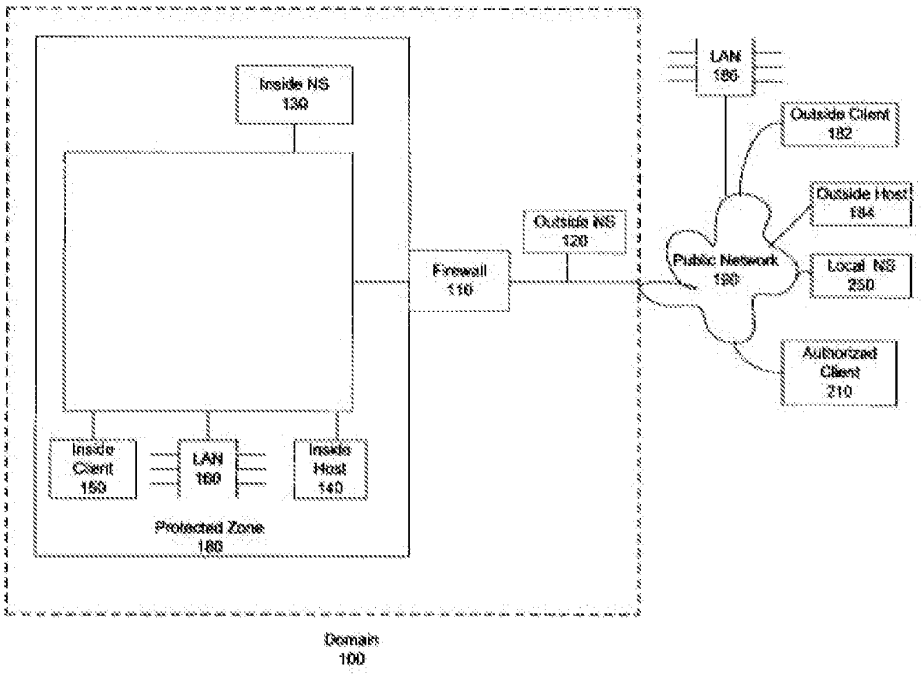
Independent claim 1 is representative of all independent claims, as discussed above. Similarly, the features of independent claim 1 have been discussed.

Also as discussed, all limitations in claim 1 are admitted prior art except the final limitation "to comprise an indication that the domain name service system supports establishing a secure communication link."

Nonetheless Aziz teaches all the limitations in representative claim 1. Aziz describes a "secure domain name server for a computer network," where the "domain name database stores secure computer network addresses for the computer network." (Abstract).

Regarding the limitation "domain name service configured for connection to a communication network," see the Aziz abstract, as discussed above. See also Fig. 1, reproduced below, which illustrates the outside name server 120 (NDS) connected to public network 190.

Fig. 1



Regarding the limitation "to store a plurality of domain names and corresponding network addresses" then "to receive a query for a network address," Aziz teaches at col. 1, ll. 26-38:

> In the Internet world, the names and addresses of hosts are stored in databases on computers located throughout the world. A computer that has one of these databases, and responds to queries for a host's address, is known by various names, including "Domain Name Server" or simply "name server." Because so many host computers have Internet addresses, it is not practical to maintain the name and address information for all hosts in one database. Instead, such information is distributed among the Internet Domain Name Servers throughout the world.
>
> Domain Name Servers and their associated name and address databases are just one system used to respond to address queries (also referred to as "resolving addresses").

Regarding the limitation to provide an "indication that the domain name service supports establishing a secure communications link," Aziz describes configuring the DNS to respond to requests with a special record that includes information needed for secure communications:

> The registered name server for a domain is configured to return a new resource record type, herein called an SX record, in response to requests for information needed for secure communications with protected hosts in that domain. The resolver on (or otherwise associated with) the authorized client is configured to use the data in the SX record to dynamically update the information used by the client to handle secure communications.
>
> (Col. 4, ll. 8-16).
>
> Alternatively, a name server can be configured to return an SX record in the response that includes the answer to a query for some other record. For example, if the client queries for a host address, a name server might send a response with the host address in the answer section and the SX record in the additional section.

(Col. 4, ll. 44-49).

Thus, the presence of SX records in the response from the DNS (NS 120) provides an indication that the DNS establishing a secure communication link.

Aziz describes automatically adding the KEY and SIG records, which also provides "an indication...." as recited in the claim. (Request at 19).

Incorporation by Reference

Thus, the third party requester proposed rejection of the claims identified above on pages 11, 12, 17-20, 32, 33 and Exhibit F-2 (claim chart), are adopted and incorporated by reference.

2.H. Rejections Based upon Kiuchi and Pfaffenberger (Issues 16-18, 20, 21)

Claim Rejections - 35 USC § 103

(Issue 16) Claims 1-4, 6, 8, 9, 14-19, 22, 24-30, 33, 34, 36-43, 46, 48-54 and 57-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiuchi in view of Pfaffenberger.

(Issue 17) Claims 5, 23 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiuchi in view of Pfaffenberger as applied to the respective, parent claims above and further in view of Rivest.

(Issue 18) Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kiuchi in view of Pfaffenberger as applied to the respective, parent claims above and further in view of Borella.

(Issue 20) Claims 20, 21, 35, 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiuchi in view of Pfaffenberger as applied to the respective, parent claims above and further in view of Broadhurst.

(Issue 21) Claims 31, 33, 35 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiuchi in view of Pfaffenberger as applied to the respective, parent claims above and further in view of Ludwig.

Summary

Independent claim 1 is representative of all independent claims, as discussed above. Similarly, the features of independent claim 1 have been discussed.

Also as discussed, all limitations in claim 1 are admitted prior art except the final limitation “to comprise an indication that the domain name service system supports establishing a secure communication link.”

Nonetheless, Kiuchi in view of Pfaffenberger teaches all the limitations in representative claim 1. Kiuchi describes a "closed HTTP-based network" ("C-HTTP”) on the Internet that relies in part upon a "C-HTTP name server." Abstract.

Regarding the limitations directed to a domain name service configured for connection to a communication network, storing a plurality of domain names and corresponding network addresses, then receiving a query for a network address, Kiuchi states at p. 65, section 2.3, subsections (2) and (3):

> A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection form the client-side proxy. 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. If it is not permitted, it sends a status code which indicates an error…When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy's public key....

The same section of Kiuchi cited above also teaches providing an indication that the domain name service supports establishing a secure communications link. Specifically, the sending of the "public key" is an indication that the domain name service (C-HTTP name server) supports the establishment of subsequent, secure communication link using a shared public key for encryption/decryption.

Pfaffenberger also describes indicating support for a secure communication link by providing a visible icon on an http browser (Request, pp. 22-24) and that the addition of an http browser to the C-http system of Kiuchi would have been obvious (p. 22).

Incorporation by Reference

Thus, the third party requester proposed rejection of claims identified above on pages 11, 12, 20-24, 33, 34 and Exhibit F-3 (claim chart), are adopted and incorporated by reference.

3. Response to Arguments

The examiner has considered the arguments and evidence of record provided in both the patent owner's Response and in the third party requester's Comments. Based on consideration of the entire record, the third party requester's arguments and evidence are deemed more persuasive. As noted in Section 1, the patent owner's Supplemental Declaration has not been entered and is not of record in this proceeding. The examiner however has briefly reviewed the Declaration, but it does not persuade the examiner to decide any issues favorable to patentability.

The patent owner appears to have presented new arguments in the Response while dropping other arguments first presented in response to the ACP. The reader of this RAN is requested to consult the prosecution history, including the ACP, if "older" arguments are again presented in the patent owner's Brief, should one be filed.

3.1. Claim Interpretation

Claim 1, which is representative, broadly recites (emphasis added):

> 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**.

Thus, claim 1 recites a domain name service ("DNS") "system" and not a particular computer device or structural configuration, such as a single secure DNS server. Such an interpretation is consistent with the specification of the patent under reexamination, *see, e.g.*, col. 40, ll. 18-31, where the DNS system is implemented using gatekeeper 2603, DNS proxy 2610 and DNS server 2609. The examiner agrees with the requester, who notes the "DNS system according to the claims can be distributed across multiple computer systems…." (Fratto Declaration, filed June 25, 2012, paragraph 31). Thus, the DNS **system** is reasonably interpreted as comprising a single device or multiple devices.

The patent owner characterizes the invention as a special and separate DNS device that traps DNS queries, determines whether the query is from a "special type of user," and then actively assists in the creation of a virtual private network ("VPN") link. *See* the original Declaration of Angelos D. Keromytis, Ph.D., filed on June 5, 2012 (the "Keromytis" declaration), ¶ 17-19.

Regarding whether a DNS device or devices are separate, as discussed above, the claims do not recite a particular special DNS device, much less a device physically separate from a conventional DNS server, which is also consistent with the specification of the patent under reexamination. Indeed in one embodiment, the patent owner states "It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience." (Col. 40, ll. 27-31, emphasis added).

In view of the above, the claimed DNS "system" is interpreted reasonably broad consistent with the specification to comprise a single device (*e.g.*, a DNS server) or various combinations of multiple devices (*e.g.*, a DNS server and other DNS devices) (*e.g.*, a DNS server, a DNS proxy) (*e.g.*, a DNS server, a DNS proxy, and other DNS devices).

Regarding whether the DNS system determines the query is from a special user and then actively assists in the establishment of a VPN, the patent owner asserts the special DNS server 2602 (Fig. 26) in the patent under reexamination differs from a conventional DNS server in that "DNS proxy 2610 [part of DNS server 2602]… determines whether the computer 2601 is authorized to access the site" and, if so, "transmits a message to gatekeeper 2603 to facilitate the creation of a VPN link between computer 2601 and secure target site 2604". (Original Keromytis Declaration, ¶ 18). "DNS proxy 2610 then responds to the computer's 2601 DNS request with an address received from the gatekeeper 2604." *Id.* That is, rather than conventionally returning a public key to the initiator (e.g., computer 2601) so that the target and the initiator can establish a VPN, the special DNS server authenticates the request, then relies upon the services of a gatekeeper to receive an address (*e.g.*, a "hopblock" address, col. 39, 67 – col. 40, l. 8) that the DNS server then provides to the initiator so that the initiator and target can establish a VPN. *See also* said original Keromytis Declaration, paragraph 19.

The claims however do not recite a DNS "server" (as previously discussed) much less a DNS server that authenticates a user and relies upon the services of a gatekeeper, which is also consistent with the specification. Indeed in one embodiment, the patent owner states the DNS

server (SDNS 3319) is queried "in the clear" (without using a VPN link) and without authenticating the user. (Col. 51, ll. 37-50). The server then replies without the use of a gatekeeper 3314 "in the clear" so that the initiator and the target can establish a VPN. *Id.*

In view of the above, the claimed DNS system is interpreted reasonably broad consistent with the specification has not requiring a DNS server capable of authenticating the user and not requiring the services of a gatekeeper to aid in the establishment of a VPN.

The district court in related litigation interpreted "indication" as having no special meaning in view of the specification of the patent under reexamination and indeed the specification does not use this term specifically. Thus, the term may be construed broadly to mean a visible message or signal to a user that the DNS system supports establishing a secure communication link. Markman Claim Construction Order, April 25, 2012, p. 27, *Virtnetx Inc. v. Cisco Systems, Inc.*, Case No. 6:10-CV-417, District Court for the Eastern District of Texas. Attached as Ex. A. to the Comments on the Action Closing Prosecution, filed September 20, 2012, in related reexamination proceeding 95/001,788.

Moreover, the Larson patent under reexamination states:

> Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device such as a keystroke entered on a keyboard or a click entered through a trackball. **Alternatively**, the **secure link is automatically established as a default setting at boot-up of the computer** (i.e., **no click**).

(Col. 48, ll. 60-66).

Thus, the "specification envisions alternative methods of activating a secure communication link other than clicking a hyperlink, which is necessarily visible...Neither the specification nor the claim language provides a basis for limiting 'indicating' to a visual indicator." (*Markman* at 27). Indeed, the Larson patent discloses an embodiment (quoted above), where the secure link is "automatically established as a default setting at boot-up of the computer...." (Col. 48, ll. 60-66). In such an embodiment, it would be reasonable to interpret the "indication" (that the DNS among other systems associated with the computer supports establishing a secure communication link) to read on 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.

3.2. Response to Patent Owner and Third Party Requester Comments Regarding Claim Interpretation

3.2.A. Domain Name Service System

The patent owner asserts the "office construes a 'DNS system' and interprets a 'DNS device' as having no bounds whatsoever...." (Response at 3). The examiner's claim analysis immediately above however, which was repeated from the last Office action, does no such thing.

The patent owner states the "office relies on the '211 patent's description of gatekeeper 2603, DNS proxy 2610, and DNS server 2609 to support its unreasonable interpretation of a

DNS system. However, the '211 patent discloses significant DNS functionality and coordination between these devices in acting upon a DNS request." (Response at 3, 4) (*See also* the original Keromytis Declaration, ¶¶ 16-19).

The claims however do not recite these specific components. Claim 1 recites a DNS "system" and not a particular device or structural configuration. For example, one part of the '211 specification describes a DNS system implemented using gatekeeper, proxy and server (col. 40, ll. 18-31) while another part of the specification describes a DNS system using one server (col. 40, ll. 27-31). In view of the above, the claimed DNS "system" is interpreted reasonably broad consistent with the specification to comprise a single device (*e.g.*, a DNS server) or various combinations of multiple devices (*e.g.*, DNS server, DNS proxy, and other DNS devices). As for unclaimed coordination between the devices, the '504 specification describes the DNS server (SDNS 3319) queried "in the clear" (without using a VPN link) and without authenticating the user (Col. 51, ll. 37-50). The server then replies without the use of a gatekeeper 3314 "in the clear" so that the initiator and the target can establish a VPN (*Id.*). There is no clear reason to read embodiments describing an ambiguous amount of coordination between multiple devices into the claims at the expense of excluding embodiments describing a single DNS device apparently coordinating very little with other DNS devices.

The patent owner apparently de-emphasizes the disclosed embodiment, discussed above, where the single DNS server 3313 may both accept and respond to a query "in the clear" with very little involvement from other DNS devices. Regarding Col. 51, ll. 37-50, the patent owner asserts this embodiment refers to Fig. 34, step 3410. "However, the '211 patent discloses that in

the immediately preceding step of Fig. 34, the SDNS 'accesses VPN gatekeeper 3314 for establishing a VPN communication link.' Only after this, in step 3410, is an address returned in two alternative scenarios: either via an administrative VPN or 'in the clear,' it does not matter which....[T]his embodiment…actively liaises with gatekeeper 3314 to establish a VPN communication link…." (Response at 11).

The patent owner incorrectly characterizes this embodiment. The SDNS does not return a secure URL after it has already coordinated with the VPN as alleged by the patent owner.

> **Alternatively**, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, **without** using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS 3319. Because the **initial communication link** in this situation **is not** a VPN communication link, the **reply** to the query can be "**in the clear**." The querying computer **can use the clear reply** for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply.

(Larson at col. 51, ll. 37-50) (emphasis added).

Thus, in this embodiment, the SDNS receives and returns a query "in the clear" before establishing a VPN.

Figs. 33 and 34, to which this paragraph refers, are reproduced below.

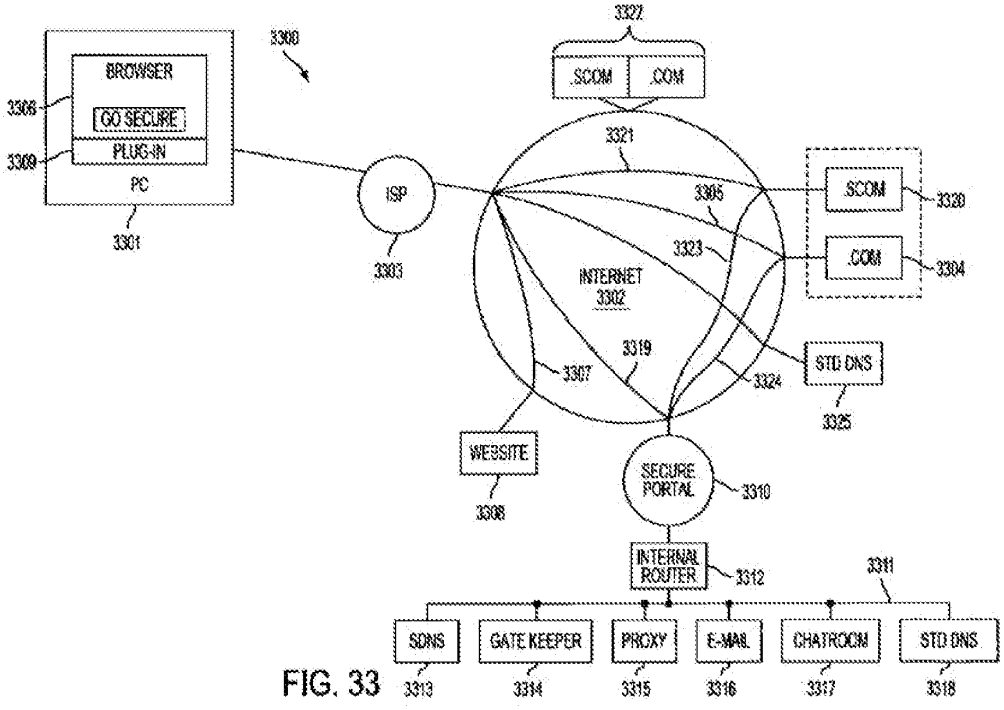

3322
.SCOM
.COM
3321
3300
BROWSER
GO SECURE
PLUG-IN
PC
3306
3309
3301
ISP
3303
3305
3323
INTERNET
3302
.SCOM
3320
.COM
3304
3319
3307
3324
STD DNS
3325
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
SDNS
GATE KEEPER
PROXY
E-MAIL
CHATROOM
STD DNS
3313
3314
3315
3316
3317
3318

FIG. 33

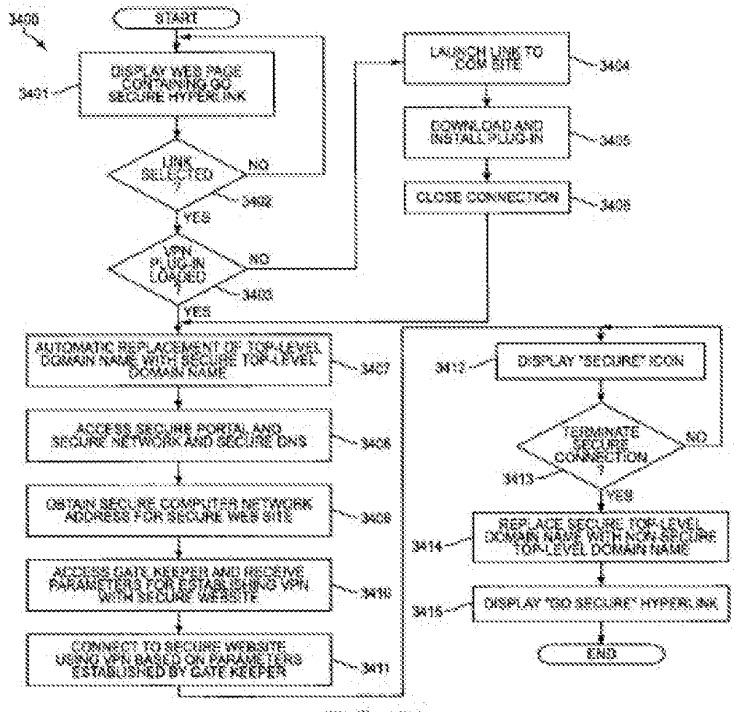

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED
NO
YES
3402
VPN PLUG-IN LOADED
NO
YES
3403
LAUNCH LINE TO COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE PORTAL AND SECURE NETWORK AND SECURE DNS
3408
OBTAIN SECURE COMPUTER NETWORK ADDRESS FOR SECURE WEB SITE
3409
ACCESS GATE KEEPER AND RECEIVE PARAMETERS FOR ESTABLISHING VPN WITH SECURE WEBSITE
3410
CONNECT TO SECURE WEBSITE USING VPN BASED ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION
NO
YES
3413
REPLACE SECURE TOP-LEVEL DOMAIN NAME WITH NON-SECURE TOP-LEVEL DOMAIN NAME
3414
DISPLAY "GO SECURE" HYPERLINK
3415
END

FIG. 34

The alternate embodiment of Col. 51, ll. 37-50 explicitly teaches that the query and response are "in the clear" before a VPN is established. Thus, step 3409 (Fig. 34) (see also col. 51, ll. 22-36) cited by the patent owner is directed to a different embodiment.

In the col. 51, ll. 37-50 embodiment relied upon by the examiner, the computer 3301 queries a single DNS server (SDNS 3313) in the clear and the server responds in the clear without the need for gate keeper 3314 to aid in the establishment of a VPN. The DNS server (SDNS 3313) only interacts with secure portal 3312 (referred to as secure portal 3310 in Fig. 33) to the extent the portal "authenticates the [user's computer] query using any well-known technique, such as a cryptographic technique…." (*Id.*). The DNS server then returns an address to computer 3301, which the computer uses to establish a VPN link to the desired domain name. Thus, a secure server merely providing conventional, authentication services for a user's computer can be considered part of the DNS system, consistent with the patent owner's specification.

3.2.B. Indication that DNS System Supports Establishing a Secure Communications Link

The patent owner argues the "Office asserts Aziz's returning of IP addresses, public keys, and authentication signatures discloses the recited indication, without explaining how doing so provides a 'visible message or signal to a user....In fact, those skilled in the art would have understood that returning IP addresses, keys, and digital signatures would not have been *visible* messages or signals *to a user.*" (Response at 5).

The examiner however notes that the providing visible messages to a user is not claimed and is not part of the examiner's claim interpretation (as was discussed above in the claim construction Section 3.1). Rather, the claims may be construed broadly to mean a visible message or signal to a user that the DNS system supports establishing a secure communication link.

The Larson patent under reexamination states:

> Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click).

(Col. 49, ll. 6-12).

Thus, the "specification envisions alternative methods of activating a secure communication link other than clicking a hyperlink, which is necessarily visible...Neither the specification nor the claim language provides a basis for limiting 'indicating' to a visual indicator." (*Markman* at 27). Moreover, the Larson patent discloses an embodiment above where the secure link is "automatically established as a default setting at boot-up of the computer...." In such an embodiment, it would be reasonable to interpret the "indication" (that the DNS among other systems associated with the computer supports establishing a secure communication link) to read on 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.

The next issue is to what extent should the DNS "supports" establishment of a communications link. The patent owner characterizes the invention as a special and separate DNS device that traps DNS queries, determines whether the query is from a "special type of user," and then actively assists in the creation of a virtual private network ("VPN") link. (Original Keromytis Declaration, ¶ 17-19). The patent owner asserts the special DNS server 2620 (Fig. 26) in the patent under reexamination differs from a conventional DNS server in that "DNS proxy 2610 [part of DNS server 2602]…determines whether the computer 2601 is authorized to access the site, and, if so, "transmits a message to gatekeeper 2603 to facilitate the creation of a VPN link between computer 2601 and secure target site 2604". *Id.* That is, rather than conventionally returning a public key to the initiator (e.g., computer 2601) so that the target and the initiator can establish a VPN, the special DNS server authenticates the request, then relies upon the services of a gatekeeper to receive an address (e.g., a "hopblock" address, col. 39, l. 67 – col. 40, l. 8) that the DNS server then provides to the initiator so that the initiator and target can establish a VPN. *See also* the original Keromytis Declaration, ¶ 19.

The claims however do not recite a DNS "server" much less a DNS server that authenticates a user and relies upon the services of a gatekeeper, which is also consistent with the specification. As discussed above in Section 3.2.A, in the embodiment of col. 51, ll. 37-50, the computer 3301 queries a single DNS server (SDNS 3313) in the clear and the server responds in the clear without the need for gate keeper 3314 to aid in the establishment of a VPN. The DNS server (SDNS 3313) only interacts with secure portal 3312 (referred to as secure portal 3310 in Fig. 33) to the extent the portal "authenticates the [user's computer] query using any well-known

technique, such as a cryptographic technique…." (*Id.*). It would thus be consistent with the specification to interpret the DNS "support" for establishing a secure communication as minimal support even including conventional query authentication.

The applied prior art teaches a DNS system that actively supports establishment of a communication link and that provides an indication it will support establishing a secure communication, such as providing a randomly generated, challenge number (Lendenmann), providing a special record that includes information needed for secure communications (Aziz), sending a public key (Kiuchi), and providing a visible icon in a http browser (Pfaffenberger).

The patent owner maintains the Larson specification "clearly and unequivocally disclaims merely returning an address or a public key by describing these actions as 'conventional' in the prior art." Response at 5. "Never does the specification equate the mere return of requested DNS records, such as an IP address or public key, with supporting secure communications." *Id.* But as discussed above, the Larson patent discloses an inventive embodiment where a query "in the clear" is authorized using "well-known techniques" at a secure portal, which then passes the query to a DNS, which returns a conventional address "in the clear." It is up to the source and target computer that then establish a secure communication themselves using the conventionally returned IP address.

Moreover, the specification of the Larson patent does not adequately disclaim even those embodiments that rely more upon the DNS actively establishing a secure communication. As discussed, claim 1 recites a domain name service ("DNS") "system" and not a particular

computer device or structural configuration, such as a single secure DNS server. The specification does not use the terms 'DNS System,' 'DNS device' and 'DNS functionality,' much less expressly define these terms to have the unique meanings advanced by the Patent Owner. Instead, the owner appears to rely on disclaimer created by general criticisms of the prior art within the specification that don't relate to the claim language as well as functional language in the claim that doesn't explicitly disclaim any embodiments. (Response at 6 & 7).

The remaining patent owner and third party requester comments are based on arguments addressed above.

3.3. Response to Patent Owner and Third Party Requester Comments Regarding Lendenmann

3.3.A Claim 1

The patent owner asserts Lendenmann does not disclose an "indication" because Lendenmann fails to provide a "visible message or signal to a user" (Response at 9 & 10), but the examiner has already addressed this claim interpretation argument in section 3.2.B.

3.3.B. "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

As discussed in the incorporated rejection, Lendenmann teaches that RCP calls rely upon well-known authentication algorithms, such as shared-secret key and public key (p. 192, section 10.4.1). The client encrypts the RPC call with the session key, which the "server immediately challenges...by sending it a randomly generated number which the client has to encrypt with the

session key and return to the server." P. 194, section 10.4.4. The client transmits the encrypted response, which the server decrypts using the server's session key obtained from the decrypted service ticket. If the decrypted random number matches, then the "session key is used in further communication over the binding." *Id.* Thus, the sending of the "randomly generated number" is an indication that the domain name service (CDS reached via a RCP call via the network) supports the establishment of subsequent, secure communication link using a shared secret key (the session key) for encryption/decryption.

By returning the network address corresponding to a secure domain name, the Cell Directory Service (CDS) also provides "an indication...." as recited in the claim. Request, Exhibit F-1 (Claim Chart), p. 13. Similarly, by only performing operations for users authorized using access control lists (ACLs), the CDS provides an indication that supports establishing a secure communication link. (*Id* at 14).

Lendenmann explicitly teaches "CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests." Lendenmann, p. 34. Thus, the cell directory service (CDS) determines whether a user is authorized for access. Indeed, the patent owner characterized DNS authorization as a distinguishing inventive feature. (Original Keromytis Declaration, ¶ 18). The Lendenmann prior art teaches a similar DNS authorization.

The patent owner responds the "ACLs are a functionality of the DCE Security Service" (Response at 10), but this does not address the ACL management software being incorporated

into all CDS clerks and servers, as explicitly taught by Lendenmann (discussed above). The CDS clerks and servers must thus perform the access checking.

The patent owner also contends "regardless of whether the ACL is part of the Security Service or part of the CDS, the CDS does nothing more than either return a network address (or binding handle), or not return one." (Response at 11). However certain embodiments disclosed in the specification of the Larson patent under reexamination do just that. For example, the patent owner's DNS proxy 2610 answers a query by "preferably using a secure administrative VPN." Larson, col. 40, ll. 19-24. Thus, Larson discloses embodiments both using a VPN and not using a VPN, although using a VPN is preferred. Thus, Larson discloses a VPN is not required to provide the answer. *See also* col. 51, ll. 48-61, where the secure DNS server 3313 receives and answers a query "in the clear" (*i.e.*, without using a VPN) by providing the requested address. The established VPN thus completely bypasses the patent owner's DNS server.

The patent owner counters the embodiment of col. 51, ll. 48-61 teaches establishing a VPN link before the address query and response (Response at 11), but this is incorrect for the reasons discussed in section 3.2.A above.

Regardless whether the returning of a secure network address can be reasonably construed as providing an indication of secure communication, the examiner agrees with the third party requester that Lendenmann teaches other features that can be so construed, as was also discussed in the last Office action. "Lendenmann teaches that specialized entries in the Cell

Directory Service, call junctions, enable the establishment of a secure communication link with registry service that manages security-related domain names....each junction 'entry contains binding information that enables a client to connect to a directory server...." (Comments at 5).

3.3.C. Binding Also Provide an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link

The patent owner argues Lendenmann teaches incomplete binding handles (*i.e.*, without security associations) (Response at 12-14), but this is explicitly contradicted by Lendenmann. "Only well-known endpoints are stored in CDS. In this case, clients obtain fully bound handles." (Lendenmann at 186).

The patent owner responds fully bound handles do not include security information (Response, 12-14), but Lendenmann explicitly teaches:

> The **binding handles are annotated with security information**. The s**erver adds the levels of security its supports** to the handles registered with its RPC runtime. **The client adds the requested security level and its own identity into the binding handle** used to contact the server. This is explained in 10.4, "RPC and Security" on page 191.
>
> (Lendenmann at 185) (emphasis added).

> The client does this with a call to *rpc_binding_set_auth_info()*, which **adds this security information to the server binding handle**. The client then uses this extended binding handle in its **further RPC calls.**
>
> (Lendemann at 191) (emphasis added).

The patent owner responds that not in all cases the binding is fully bound (Response at 12, 13), but this is not the point, as Lendenmann explicitly teaches binding handles, especially bindings comprising "well-known endpoints," are fully bound.

The patent owner also asserts the user must add to the binding handle to make it complete, but as cited above, Lendenmann teaches that the server also adds security information to the bindings. Even if only the client added security information, Lendenmann also teaches (above) that once the security information is added to the binding at the server, the server uses the binding security information for "further RPC calls." *See also* the third party requester's comments (Comments at 7).

3.3.D. Authentication Challenge also Provides an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link

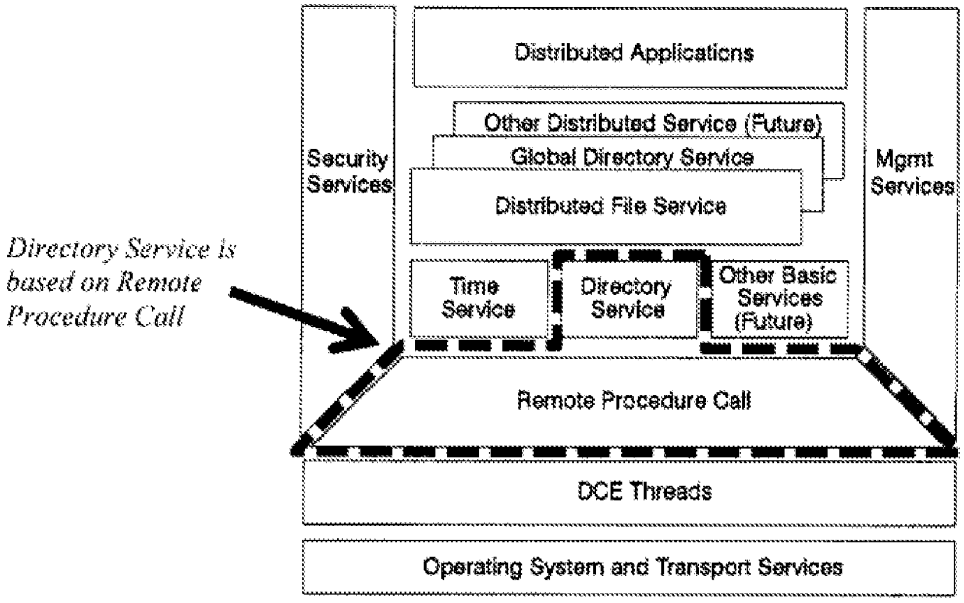
The patent owner argues the Remote Procedure Call ("RPC") authentication challenge is not related to CDS, thus the CDS does not provide the authentication challenge (indication) after the query (Response at 14, 15). *See also* the original Keromytis Declaration, ¶ 33. Fig. 3 (p. 173) of Lendenmann however illustrates that the "Directory Service" (i.e., CDS) is based upon the RPC foundation. "This chapter discusses all components involved in the execution of an RPC, including CDS and Security Services access." *Id.*

The patent owner criticizes this teaching as overly broad, but the Lendenmann statement explicitly teaches the CDS executes RPC and thus the RPC authentication challenge is related to the CDS. The patent owner counters this statement merely identifies the CDS and security

services as components of the RPC, not that the server communicates via the RPC (Response at 14). The statement however provides the CDS (part of the server) executes RPC.

The patent owner also alleges that other parts of the Lendenmann disclosure teach no relationship between CDS and RPC as it relates to authentication, for example, CDS relies upon DCE rather than RPC (Response at 14 and 15). As noted by the third party requester however, Lendenmann elsewhere consistently teaches that CDS uses RPC. For example Lendenmann states the RPC "is used by most of the other DCE technology components for their network communications." (Lendenmann at 9).

The examiner agrees with the third party's annotation of Lendenmann, Fig. 3, which is reproduced below and which illustrates the DCE (Cell Directory Service) relies upon RPC:



Lendenmann Fig. 3 (Annotated)

The third party requester also notes that's the patent owner's argument that the CDS communicates with the client using a client-server model contradicts Lendenmann, which teaches the CDS uses a "data-sharing model" that uses RPC to communicate over a network.

> In data sharing, the data of the server are sent to the client. … In OSF DCE, **data sharing is built upon RPC**, which is used as the means of transferring data. Both the **Directory Service** and the Distributed File System are **based upon the data-sharing model**.

(Lendenmann at 9) (emphasis added).

3.3.E. Independent Claims 36 and 60

The patent owner sets forth arguments (Response at 16) previously addressed above in regard to claim 1.

3.2.F. Dependent Claims 5, 23 and 47

The patent owner's arguments are based on the premise that the security service is not separate from the CDS and that queries to the CDS do no use RPC, however this view was addressed by the examiner in section 3.3.B and D above.

The patent owner also alleges the examiner does not assert encryption is involved with the ACL and that the examiner mistakenly believes "communications with a CDS occurs via RPC and that the various potential security features of RPC allegedly apply to communications between a client and CDS." (Response at 16).

As noted by the requester however (Comments at 9, 10), the patent owner has not addressed the rejections, which explain a query from a client to a directory service (CDS) server is made by a RPC, as illustrated in Fig. 15. Moreover, RPC calls rely upon well-known authentication algorithms, such as shared-sect key and public key including supplying the requesting client with a session key and a service ticket encrypted with the server's session key (i.e., digitally signed certificate). The client encrypts the RPC call with the session key, which the server challenges with a randomly generated number, which the client than has to encrypt with the session key and return to the server. (ACP at 10 and 11).

3.2.G. Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57

The patent owner's arguments are based on the premise that the CDS return only incomplete bindings, however this view was addressed by the examiner in section 3.3.C above.

3.2.H. Dependent Claims 24 and 48

The patent owner argues Lendenmann fail to teach "at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." Claims 24 and 28 "describe a functional relationship between the "at least one of the plurality of domain names" and the "domain name service system." (Response at 17 and 18).

First, Lendenmann does indeed teach that a domain names comprises an indication that the DNS system supports a secure communication link. *See, e.g.*, p. 23, "/.:/subsys/dce/sec" and "/.:/subsys/dce/sec/master." *See also* the Comments, pp. 11 & 12.

Second, if it is now the patent owner's position that the functional relationship between domain name and the DNS provides the indication rather than the name itself, then the claim permits the domain name, via the functions of domain name lookup and the resulting provision of a certificate, to provide an indication that the DNS supports establishing a secure communication link. As discussed in Sections 3.3A-C, Lendenmann teaches such a system as well.

On the other hand, if it is the patent owner's position that the name itself provides the indication, then the examiner maintains a "name" indicating that the DNS supports a secure communication link is nonfunctional descriptive material and thus cannot distinguish over the prior art. A "name" comprising an "indication" (as broadly recited) of support for a secure communications link is descriptive material directed to the mere arrangement of data. It is not a data structure (physical or logical relationships among data elements designed to support specific data manipulation functions) that defines a functional interrelationship to a secure communications function. MPEP 2106.01. In order to claim functional descriptive material, the claim should explicitly recite a data structure, such as a domain name comprising a secure top-level domain name (*e.g.*, ".scom" Larson, col. 50, ll. 25-37) and explicitly recite a functional relationship that interrelates the secure top-level domain name to the establishment of a secure communications link. See also MPEP § 2111.05(I)(A).

The examiner declines to find a domain name is patentable.

3.2.I. Dependent Claim 7
Dependent Claims 8 and 9
Dependent Claim 10

The patent owner sets forth arguments (Response at 19) previously addressed above.

3.2.J. Dependent Claims 12 and 13

The examiner agrees with the third party requester that it does not follow from the examiner's prior arguments that all TCP-based communications are VPNs nor does the requester explain the supposed difference between using a moving window and basing actions on a moving window (Comments at 12, 13).

3.3. Response to Patent Owner and Third Party Requester Comments Regarding Lendenmann in view of Ludwig

The patent owner sets forth arguments (Response at 20) previously addressed above.

3.4. Response to Patent Owner and Third Party Requester Comments Regarding Aziz

3.4.A. Claim 1

Client 210 Is Part of a DNS System

The patent owner alleges the examiner's claim interpretation is overly broad because "if merely sending and receiving DNS queries qualified a network component as being a part of the alleged DNS system, then literally any network component….that can communicate over a network would be part of the alleged DNS 'system.'". (Response at 23).

The authorized client 210 in Aziz however does more than "merely sending and receiving DNS queries." The DNS system comprises authorized client 210 and the authorized client 210 directly establishes a secure communication with the target. The DNS system thus supports establishing a secure communication link. Specifically, the DNS system is not limited to NS 120, as discussed above (see also Section 3.1). Indeed, the query initiator (authorized client 210) comprises a resolver program (name server software). (Col. 6, l. 61 – col. 7, l. 7 and col. 8, ll. 28-32). The resolver is also part of the DNS system because the resolver performs the following functions: "(1) return the answer to the query if it is available locally; otherwise, (2) find the best servers to ask for the answer, (3) send queries to the servers until one responds; and (4) process the response." *Id.* The resolver thus also caches the response locally in order to minimize the number of queries it has to send to name servers. Thus, the query initiator (e.g., authorized client 210) is part of the DNS system. The query initiator however also establishes the secure communication link with the target (e.g., inside host 130 and firewall 110).

Returning the Address of a Firewall via a SX Record Provides an Indication that the DNS Supports Establishing a Secure Communication

Assuming incorrectly for the sake of argument client 210 is not part of the DNS system, Aziz still teaches that the DNS system (including Fig. 1, local name server 250, outside name server 120, firewall 110, and inside name server 130) supports the establishment of a secure communication link. Aziz teaches providing an "indication" that the DNS system supports a secure communication link, such as by releasing the SX, KEY and SIG records.

Considering only the SX record for the moment (the KEY and SIG records will be addressed in the subsequent section), Aziz explicitly teaches that releasing the address of firewall 110 (SX record) provides an indication that the DNS system supports a secure communication link (col. 5, l. 32 –col. 6, 46) (emphasis added):

> Given the system architecture just described, what happens when application 215 running on authorized client 210 **wants to communicate securely** with protected host 140 in protected zone 180? **Before application 215 can do so, it needs outbound secure message information.** This information, stored on authorized client 210, may include the address of inside host 140, the **address and key of firewall 110**, and the cryptographic protocols to use.
> ....
> according to various embodiments of the invention, the **problem is solved** by enabling authorized clients to dynamically update their outbound secure message information **using information that is stored and maintained in a central location**.
> ....
> The data field of the **SX record contains** the identifier (e.g., n**ame or address) of a "secure exchanger"** associated with the owner of the record. A secure exchanger is a machine that handles secure communications for itself or for another machine (e.g., performs encryption or decryption).
> ....
> Because a firewall frequently performs the secure exchanger function, the term "**firewall 110" will be used herein to refer to a secure exchanger**.
> .....
> Alternatively, a **name server can be configured to return an SX record** in the response that includes the answer to a query for some other record.

Thus in Aziz, the DNS system (comprising NS 120) provides an "indication" in the form of an address of firewall 110 to which a secure communication link is established. The other information providing the "indication" (public keys, digital signature) is discussed in the next section. The DNS system itself provides an indication of support for secure communication by providing information (firewall address, keys, and digital signature) necessary for the query initiator to establish the secure communication with the target. This interpretation is also consistent with the specification of the Larson patent under reexamination, which teaches a DNS system that provides an address to the query initiator so that the initiator can establish a secure communication link to the target bypassing the DNS. For example, the Larson patent under reexamination discloses an embodiment at col. 51, ll. 21-50 (emphasis added):

> SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website.
> ....
> **Alternatively**, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS 3319. Because the initial communication link in this situation is not a VPN communication link, the reply to the query can be "in the clear." **The querying computer can use the clear reply for establishing a VPN link to the desired domain name.** Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply.

Thus, in one embodiment of the Larson patent under reexamination, the DNS system (SDNS 3313) provides an address to the query initiator "in the clear" so that the initiator can establish a secure communication link (VPN) to the target (web site corresponding to the secure domain name, *e.g.*, server 3322) bypassing SDNS 3313.

The biggest structural difference between the Larson and Aziz teachings discussed above is that, in Larson, SDNS 3313 "authenticates" the query however this feature is not recited in the independent claims. *See, e.g.*, dependent claim 5, which for the first time recites "authenticate the query..." thus implying by claim differentiation that parent, independent claim 1 need not be interpreted as requiring such an unclaimed feature. Nonetheless, as discussed above, Aziz teaches the query initiator is an "authorized" client 210.

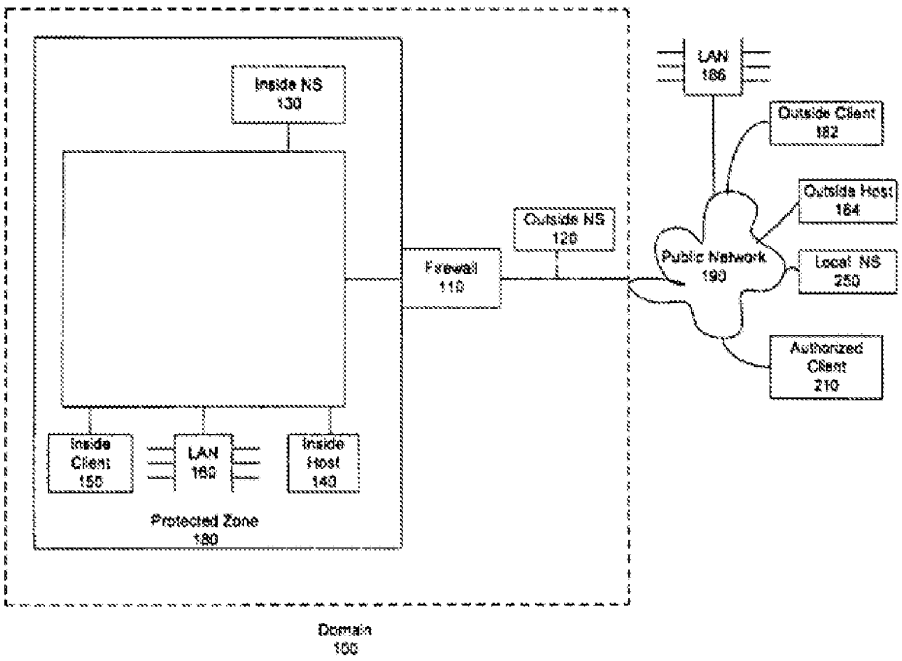
This and other teachings to be discussed in Aziz are hardly directed to a "conventional DNS system." Moreover, prior art may anticipate or render obvious a broadly claimed invention regardless of whether the prior art describes "conventional" technology.

The patent owner counters the "SX record is returned to authorized client 210 based merely on whether the SX record exists for a particular host name, and regardless of whether authorized client 210 supports establishing a secure communication link." (Response at 24).

As discussed above though, a SX record contains an identifier (e.g., name or address) of a "secure exchanger" associated with the owner of the record. A secure exchanger is a machine that handles secure communications for itself or for another machine (e.g., performs encryption

or decryption). The SX record provides an indication that establishment of a secure communication link via the secure exchanger is supported.

The examiner also agrees with the third party requester, who notes the Aziz secure DNS system further includes inside name server 130 and firewall 110.



Aziz Fig. 1

In one embodiment, authorized client 210 requests from NS 120 the address of inside host 140. Instead, the authorized client 210 is given a SX record indicating firewall 110 acts as the secure exchanger for inside name server (NS) 130. The response thus indicates NS 130 (part of the DNS) is capable of establishing a secure communication link via the secure exchanger (firewall 110). "Aziz is not merely returning requested resources…. the authorized client sent a

query requesting the IP address for inside host 140…outside NS 120 provides the SX record with information usable to establish a secure communication link with another name server." Comments at 16) (*See also* Aziz at col. 12, ll. 1-20).

Returning Public keys and Digital Signatures via KEY and SIG Records Provides an Indication that the DNS Supports Establishing a Secure Communication

As discussed, the DNS system comprises authorized client 210 and the authorized client 210 directly establishes a secure communication with the target. The DNS system thus supports establishing a secure communication link.

Assuming incorrectly for the sake of argument client 210 is not part of the DNS system, Aziz still teaches that the DNS system (including Fig. 1, local name server 250, outside name server 120, firewall 110, and inside name server 130) supports the establishment of a secure communication link. Aziz also teaches providing an "indication" that the DNS system supports a secure communication link, such as by releasing the SX, KEY and SIG records.

Considering only the KEY and SIG records for the moment (the SX record was addressed above in section 3.3.B), Aziz explicitly teaches that releasing a public key and digital signature provides an indication that the DNS system supports a secure communication link (col. 5, l. 62 - col. 6, l. 10) (emphasis added).

> To **support the need for secure communications**, a version of the Internet Domain Name System ("secure DNS") uses security extensions including KEY and SIG resource record types. The KEY resource record can be used to **distribute public keys** and associated information. That is to say, a KEY record could

> contain a key, a key name, or an algorithm. The SIG, or "signature," resource record can be used to **authenticate the data in other resource records**. One of the data fields in a SIG record is the "labels" field. This field is the count of how many labels are in the original SIG record owner name as it appears in the zone database (e.g., *.sun.com. has two labels because the null label (".") for root and the wildcard ("*") are not included in the count). This label count can, therefore, be used to derive the original name of a record that was retrieved as the result of wildcard substitution (to be described in detail later). The original name is needed, for example, to verify a digital signature.

Thus, the DNS system itself provides an indication of support for secure communication by providing information (key and digital signature) necessary for the query initiator to establish the secure communication with the target. This interpretation is also consistent with the specification of the Larson patent under reexamination, which teaches a DNS system that provides an address to the query initiator so that the initiator can establish a secure communication link to the target bypassing NS 120. *See* Section 3.3.B above for additional details.

The biggest structural difference between the Larson and Aziz teachings discussed above (*see also* Section 3.2.A) is that, in Larson, SDNS 3313 “authenticates” the query however this feature is not recited in the independent claims. *See, e.g.*, dependent claim 5, which for the first time recites "authenticate the query..." thus implying by claim differentiation that parent, independent claim 1 need not be interpreted as requiring such an unclaimed feature. Nonetheless, as discussed above, Aziz teaches the query initiator is an "authorized" client 210.

This and other teachings to be discussed in Aziz are hardly directed to a "conventional DNS system." Moreover, prior art may anticipate or render obvious a broadly claimed invention regardless of whether the prior art describes "conventional" technology.

The patent owner counters the that KEY and SIG records are returned "based merely on whether the SX record exists for a particular host name, and regardless of whether authorized client 210 supports establishing a secure communication link." (Response at 24).

As discussed above though, the KEY and SIG record contain public encryption keys and authentication data, which are used to establish a secure communication via client 210. The KEY and SIG records thus provides an indication that establishment of a secure communication link via the secure exchanger is supported.

The examiner also agrees with the third party requester, who again notes that, similarly to SX records, KEY and SIG records are used to establish secure communication links with other DNS devices, such as firewall 110 and inside NS 130.

Building Tunnel Information Tables Provides an Indication that the DNS Supports Establishing a Secure Communication

The patent owner asserts that building information used for secure communications in the resolver program, such as tunnel information tables, fails to provide an indication that the DNS system supports establishing a secure communication link because the client 210 is separate from the DNS system. Rather Aziz teaches a conventional DNS system. (Response at 27 & 29).

As discussed in section 3.4A above, the premise of the patent owner's argument is incorrect. The DNS system comprises authorized client 210 because client 210 executes a DNS resolver program. The authorized client 210 (part of the DNS system) then directly establishes a secure communication with the target. The DNS system, comprising the client, thus supports establishing a secure communication link and the prerequisite information, such as tunnel information table residing in the client, provides an indication that the secure communication will be established.

RFC 2065 (DNS-sec) Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

Aziz teaches the security extension to DNS ("DNS-sec") (RFC 2065) in one embodiment is used to distribute the KEY and SIG records. Col. 6, ll. 11-21. Thus, the patent owner's arguments (Response at 28 & 29) are unpersuasive for the reasons discussed above, which addressed the distribution of KEY and SIG records. The assertion that the host speaks IPSEC bit in the KEY record provides an indication of support for the establishment of secure communication with the host. The IPSEC bit independently provide the "indication," but the KEY record as a whole also provides the recited indication, as discussed above. The patent owner argues for a distinction between whether the "host speaks using a particular security protocol" and indicating that a "domain name service system supports establishing a secure communication link." (Response at 28). A bit that indicates the host speaks IPSEC however does provide the broadly recited "indication" of support for secure communication. The patent owners arguments are directed to degrees of uncertainty not recited in the claims.

3.4.B. Independent Claims 36 and 60
Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57

The patent owner's arguments (Response at 29) were addressed above.

3.4.C. Dependent Claims 18 and 42

The patent owner contends Aziz fails to teach a domain name reserved for secure communication link (Response, pp. 36 & 37), but Aziz teaches "network administrator may sometimes also want to permit authorized clients outside the protected zone to communicate with hosts inside the protected zone" (col. 2, ll. 20-22), which Aziz achieves by use of a firewall 110 to handle encrypted communication between an "authorized" client 210 and a host inside protected zone 180 (Fig. 1 and col. 9, ll. 5-7). A host inside the "protected zone" however corresponds to domain names, such as eng.sun.com and corp.sun.com. Col. 1, ll. 58-60. Thus, domain names, such as eng.sun.com, are reserved to a protected zone for the possibility of secure communications with an outside, authorized client, although certainly the initiator is not required to then establish a secure communication link (i.e., take advantage of the reserved domain name). The domain names are "reserved" for secure communication as the term "reserved" is understood to one of ordinary skill in the art contrary to the patent owner's assertion.

3.4.D. Dependent Claims 24 and 48

The patent owner's arguments were addressed above.

3.4.E. Dependent Claims 2, 6-9, 14, 15, 19-22, 25, 28, 34, 35, 37-39, 43-46, 49, 52, 58 and 59

The patent owner sets forth arguments (Response at 30) previously addressed above.

3.5. Response to Patent Owner and Third Party Requester Comments Regarding Aziz in view of Lawton

3.5.A. Dependent Claims 3, 4 and 26

As explained in section 3.4.A above, Aziz teaches that the SX record is returned with the address corresponding to a domain name query. See also col. 6, ll. 48-50. RFC 2065 (DNS-sec) in one embodiment is used to implement the KEY and SIG resource records. Col. 6, ll. 11-23. In DNS-sec, the public key "must be included if space is available" in a type "A" (host address) response record (section 3.7). See RFC 2065, of record in this proceeding. As also explained in sections 3.4.A, the SX and KEY records provide for the establishment of a secure communication link. Thus, in Aziz a domain name enables establishment of a secure communication link. The requester relied upon Lawton to teach publication of a protected domain name (domain name indicates the purpose of the name) so that the domain name would obviously be used enable a secure communication from outside the protected network.

The first part of the patent owner's response are based on the view that the SX, KEY and SIG records do not provide the recited indication, which the examiner addressed in section 3.4 above. (Response at 31). The patent owner also asserts the examiner mischaracterized the requester's rejection regarding referral to publication of domain names used for enable secure communication, but does not argue specifically the actual incorporated rejection is in error. (*Id.*) Regardless, the examiner referred to Lawton teaching the publication of Aziz's protected domain

names, where the Aziz names support the establishment of secure communication, which is clear in the context of the incorporated rejections. As the requester notes, the domain names of Lawson indicate the purpose of the domain name (Comments at 21), thus Aziz in combination with Lawson teaches secure domain names that indicate the purpose of the domain name (secure communication).

3.6. Response to Patent Owner and Third Party Requester Comments Regarding Aziz in view of Franaszek

3.6.A. Claim 9

The patent owner argues the combination of Aziz in view of Franaszek would have changed the principle of operation of Aziz and moreover Franaszek is nonanalogous art. (Response at 32, citing back to earlier comments). Although the examiner agrees that Franaszek is somewhat further afield than a secondary reference directed to network communications would be, Franaszek is merely being relied upon to teach organizing a plurality of communication paths (which are taught by Aziz) into a hierarchy. Such a broad concept - the need to organize communication paths into a hierarchy – is applicable to both communication networks and computer networks. Moreover, this broad concept, when added to Aziz, does not require Aziz to change its principle of operation. The communication networks taught by Aziz alone would simply be organized hierarchically after the modification. The patent owner also asserts Franaszek is nonanalogous art because it is not reasonably pertinent to the problem recited in the claim of the patent under reexamination, however this is unpersuasive this problem - a need for "easy and convenient" communications - is not claimed, and thus the patent owner's

arguments are essentially directed to unclaimed features. (Response at 32). The examiner nonetheless agrees with the requester's additional explanation of how Franaszek is pertinent. (Comments at 22).

3.6.B. Dependent Claim 10 Dependent Claims 29-32 and 53-56

The patent owner sets forth arguments (Response at 32 & 33) previously addressed above.

3.7. Response to Patent Owner and Third Party Requester Comments Regarding Kiuchi and Pfaffenberger

3.7.A. Claim 1, 36 and 60

The patent owner's assertions are couched in terms that suggest the examiner never applied his claim interpretation to the prior art. (Response at 33). The patent owner's arguments however actually appear to implicate the examiner's claim interpretation as mistaken for failing to apply the owner's preferred interpretation in this reexamination proceeding, which stress providing visible messages (or similar highly overt indications) to the user in the most direct manner possible. Such as narrow interpretation is neither reasonable nor consistent with the patent owner's specification. *See* sections 3.1 and 3.2 above.

Returning a Public Key of a Secured Proxy Server Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner asserts returning the public key of the secure server-side proxy fails to provide an indication that the DNS system itself supports establishing a secure communication link because the secured server-side proxy is separate from the DNS system. Rather, Kiuchi teaches a conventional DNS system. (Response at 34 and 35). *See also* the original Keromytis Declaration, ¶ 56 & 57.

The examiner does not agree. Kiuchi teaches providing an "indication" that the DNS system supports a secure communication link, such as by releasing the public key, nonce value and IP address of the secured, server-side proxy.

Considering only the public key or the moment (the IP address will be addressed in the subsequent section), Kiuchi explicitly teaches that releasing the public key of the secure server-side proxy provides an indication that the DNS system supports a secure communication link (p. 65, section 2) (emphasis added):

> A client-side proxy **asks** the C-HTTP name server **whether it can communicate** with the host specified in a given URL. **If the name server confirms that the query is legitimate**, it examines whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection from the client-side proxy. 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**. If it is not permitted, it sends a status code which indicates an error. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy.

Thus in Kiuchi, the DNS system (comprising the C-HTTP name server) provides an "indication" in the form of public key of a secure server-side proxy to which a secure communication link is established. The other information providing the "indication" (IP address and nonce values) is discussed in the next section. The DNS system itself provides an indication of support for secure communication by providing information (public keys, IP address, nonce values) necessary for the query initiator to establish the secure communication with the target. This interpretation is also consistent with the specification of the Larson patent under reexamination, which teaches a DNS system that provides an address to the query initiator so that the initiator can establish a secure communication link to the target bypassing NS 120. For example, the Larson patent under reexamination discloses an embodiment at col. 51, ll. 21-50 (emphasis added):

> SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website.
> ....
> **Alternatively**, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, **without** using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS 3319. Because the **initial communication link** in this situation **is not** a VPN communication link, the **reply** to the query can be "**in the clear**." The querying computer **can use the clear reply** for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply.

Thus, in this embodiment, the SDNS receives and returns a query "in the clear" before establishing a VPN.

Figs. 33 and 34, to which this paragraph refers, are reproduced below.

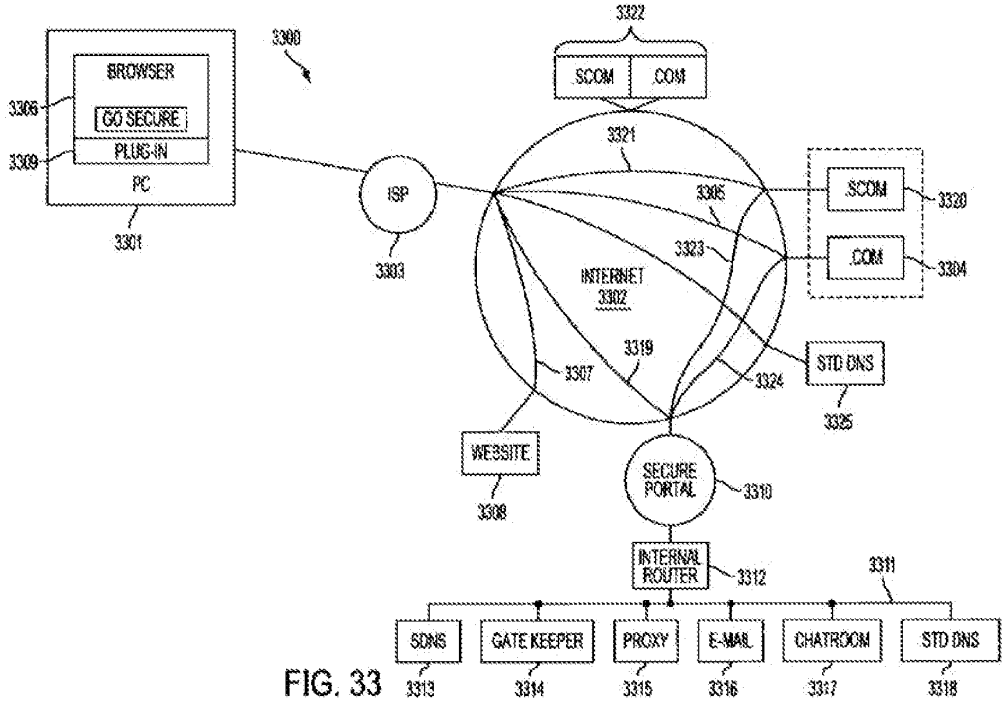


FIG. 33

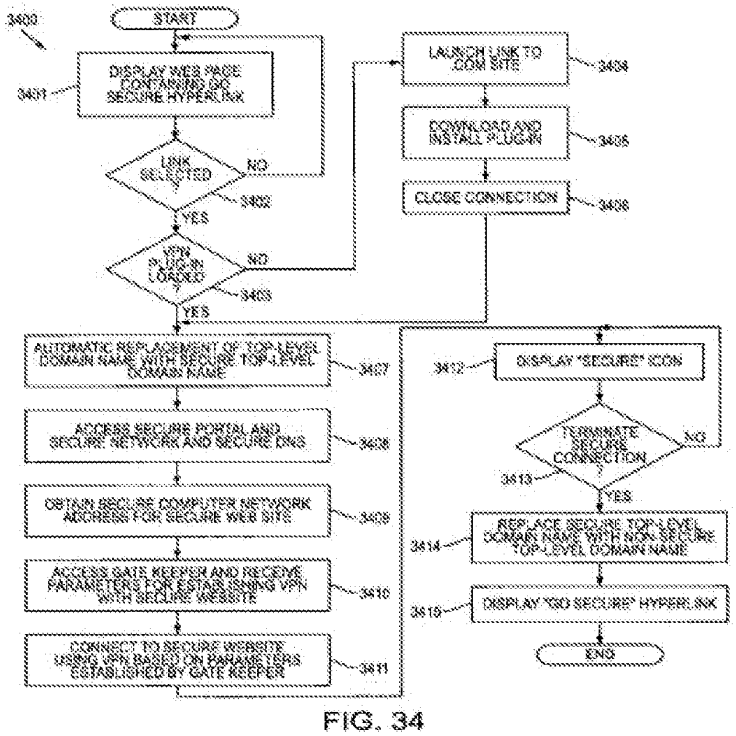


FIG. 34

The alternate embodiment of col. 51, ll. 37-50 explicitly teaches that the query and response are "in the clear" before a VPN is established. Thus, step 3409 (Fig. 34) (see also col. 51, ll. 34-48) cited by the patent owner is directed to a different embodiment.

In the col. 51, ll. 37-50 embodiment relied upon by the examiner, the computer 3301 queries a single DNS server (SDNS 3313) in the clear and the server responds in the clear without the need for gate keeper 3314 to aid in the establishment of a VPN. The DNS server (SDNS 3313) only interacts with secure portal 3312 (referred to as secure portal 3310 in Fig. 33) to the extent the portal "authenticates the [user's computer] query using any well-known technique, such as a cryptographic technique…." (*Id.*). The DNS server then returns an address to computer 3301, which the computer uses to establish a VPN link to the desired domain name. Thus, a secure server merely providing conventional, authentication services for a user's computer can be considered part of the DNS system, consistent with the patent owner's specification.

Thus in one embodiment of the Larson patent under reexamination, the DNS system (SDNS 3313) provides an address to the query initiator "in the clear" or encrypted so that the initiator can establish a secure communication link (VPN) to the target (web site corresponding to the secure domain name, *e.g.*, server 3322) bypassing SDNS 3313.

There appears to be no significant structural difference between the Larson and Kiuchi teachings discussed above. Indeed, both teach that the name server authenticates the query, although this feature is not specifically claimed until dependent claim 5.

This and other teachings to be discussed in Kiuchi are hardly directed to a "conventional DNS system." Moreover, prior art may anticipate or render obvious a broadly claimed invention regardless of whether the prior art describes "conventional" technology.

The patent owner maintains the Larson specification disclaims merely returning an address or a public key by describing these actions as 'conventional' in the prior art." (Response at 36). The examiner was not persuaded by the assertion however, as discussed in this section and Section 3.2.A above.

The requester correctly notes that the DNS system itself participates in a secure communications link, although such a direct participation is not required according to a reasonably broad interpretation of the claims consistent with the specification, as discussed above in this section. (Comments at 24). The requester also correctly notes that the Larson patent under reexamination teaches bypassing the name server when establishing a secure communication (as also discussed above in this section), therefore it is not necessary to interpret the claims as requiring a secure communication between the name server and user. (*Id.*).

Returning a IP Address of a Secured Proxy Server and Nonce Value Both Teach an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner offers similar reasons to those addressed above as to why the IP address fails to provide the claimed indication (e.g., claim interpretation consistent with the specification and disclaimer). (Response at 37 & 38). *See also* the original Keromytis Declaration, ¶ 58. The examiner finds the present arguments unpersuasive for similar reasons. The examiner notes that the release of the IP address by the C-HTTP name server cannot be viewed in isolation as a conventional domain name query for an IP address. As discussed above, Kiuchi teaches that if a connection to the secure server-side proxy corresponding to the IP address, then the C-HTTP releases an error code and subsequently performs a conventional DNS lookup. Thus, the release of the IP address is in the context of an unconventional DNS lookup for the purpose of determining whether the DNS system can support establishing a secure communication link by releasing the necessary public key, IP address, and nonce value.

The patent owner also asserts "Kiuchi does not teach that the C-HTTP name server (the alleged DNS system) requests the subsequent DNS lookup outside of the outside of C-HTTP. Instead, it is the client-side proxy that runs the lookup if it receives an 'error status' from the C-HTTP server…." (Response at 38). The patent owner's argument however is premised on limitation the claimed DNS "system" to just one device, the C-HTTP name server, which the examiner does not do.

Kiuchi's C-HTTP Name Server Stores Domain Names and Corresponding Network Addresses

The patent owner presents for the first time a detailed argument that C-HTTP fails to send the IP address of the server-side proxy in response to a query because the URL used for the query "does not correspond to the server-side proxy but to the resource itself located on an origin server." Rather, it is argued, the client-side proxy "takes the connection ID and forwards, the stripped, original resource name to the server…." (Response at 39). The patent owner argues the C-HTTP name service request includes a field "SERVER-SIDE-PROXY-NAME," but one of ordinary skill in the art would believe this field refers to the URL of the resource on the origin server, not to the domain name of the server-side proxy. (*Id.*).

The examiner however agrees with the third party request, who notes a specific type of "correspondence" between the URL (domain name) and address is not claimed. Indeed, several embodiments disclosed in the patent under reexamination disclose a DNS server that does not return the IP address of the destination computer or resource (Comments at 25 and 26). Thus, the examiner does not believe there is any sound basis to read the claims in a narrow manner to exclude these embodiments.

The requester also cited to Appendix 3 of Kiuchi, which apparently illustrates the query sent to the C-HTTP name server containing the server-side proxy's domain name and the C-HTTP responds to this request with the server-side proxy's IP address. The requester's annotation of Appendix 3 is reproduced below:

Appendix 3. Examples of C-HTTP communication (a-h)

Note that lines with an asterisk are encrypted. Components of C-HTTP-based communication are as follows:

1) Client-side proxy
hostname: University of Tokyo Branch Hospital
IP address: 130.69.111.111
2) server-side proxy
hostname: Coordinating Center.CSCRG
IP address: 130.69.222.222
port number: 8080
3) C-HTTP name server:
Name Server.CSCRG
IP address: 130.69.222.111
4) User agent:
IP address: 192.168.123.123

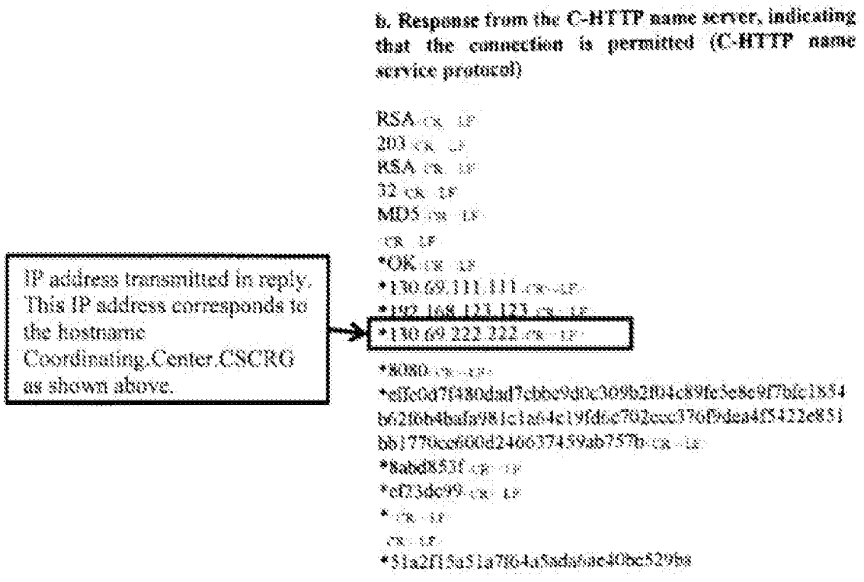
Server-side proxy's hostname

Server-side proxy's corresponding IP address

a. Lookup of server-side proxy information (C-HTTP name service protocol)

C-HTTPNS/0.1 CR LF
RSA CR LF
74 CR LF
RSA CR LF
32 CR LF
MD5 CR LF
CR LF
*SERVER CR LF
*130.69.111.111 CR LF
*192.168.123.123 CR LF
*Coordinating Center.CSCRG CR LF
*8080 CR LF
CR LF
*827ae79ba214769ea299f249bdb9aa97

Server-side proxy's domain name sent in the query to the C-HTTP name server



3.7.B. There Are No Deficiencies in Kiuchi for Pfaffenberger to Remedy

The patent owner contends Pfaffenberger fails to remedy the deficiencies in Kiuchi (Response at 39 & 40), but as discussed in sections 3.7.A above, Kiuchi is not deficient in the manner asserted by the patent owner.

3.7.C. The Combination of Kiuchi and Pfaffenberger Would Have Been Obvious

The patent owner argues the combination of Kiuchi in view of Pffafenberger would not have been obvious because Pfaffenberger is nonanalogous art because it is not reasonably pertinent to the problem recited in the claim of the patent under reexamination. (Response at 40). This argument is unpersuasive however because the asserted problem - a need for "easy and convenient" communications - is not claimed, and thus the patent owner's arguments are

essentially directed to unclaimed features. *See also* the requester's arguments as to why Pfaffenberger teaches analogous art, which the examiner agrees with. (Comments at 27 & 28).

3.7.D. Dependent Claims 8-10, 12 and 13

The patent owner refers back to an earlier Response (40 & 41). Accordingly, the examiner notes that he addressed these arguments in the ACP (49-51).

The patent raises an additional argument that Kiuchi fails to teach the C-HTTP name server is connectable to the virtual private network between the client-side proxy and the server-side proxy. (Response at 41). This assertion however depends upon incorrectly interpreting the recited DNS "system" to mean just one device – the C-HTTP name server. *See also* Section 3.1 above. See also the requester's rebuttal. (Comment at 28 & 29).

3.7.E. Dependent Claims 24 and 48

Kiuchi teaches the domain name for a secured C-HTTP host is "another.server.in.closed.network," which provides an indication that the host (server) corresponding to name (closed) is secure at least to the extent it is "closed." The name server (within the DNS system) resolves the name into an address and public key corresponding to the secure host in order to support the establishment of a connection to the secure (closed) server. The domain name therefore also indicates that a DNS system will resolve the domain name into an IP address and public key to support the establishment of a connection to the secure (closed) server.

Moreover, a domain "name" comprising an "indication" (as broadly recited) of support for a secure communications link is descriptive material directed to the mere arrangement of data. The examiner declines to find the content of a domain name patentable subject matter. *See* Section 3.2.H for further details.

The patent owner counters the "host is behind the server-side proxy firewall and separate from the C-HTTP name server" (Response at 41), but as discussed in Section 3.1 above, the claimed DNS "system" cannot be reasonably be limited to just one device. Moreover, as the requester notes (Comments at 29 & 30), the "C-HTTP name server itself has a domain name of 'Name.Server.CSCRG', (Kiuchi at 73, col. 2). This name is not valid in the general Internet domain system, and instead is valid only in the secure C-HTTP closed network."

The patent owner also argues that, regardless, no domain name in Kiuchi includes the "indication" feature because "by the time Kicuhi's alleged domain name is displayed, the C-HTTP name server has already resolved it into an address." (Response at 42). The examiner however agrees with the requester that the patent owner is now reading significant new limitations ("and wherein the indication is displayed before the domain name is resolved into an IP address") into the claim in order to distinguish over the applied prior art. (Comments at 30).

3.6.F. Dependent Claim 2-4, 6, 14-19, 22, 25-30, 33, 34, 37-43, 46, 49-54 and 57-59 Dependent Claims 5, 23, and 47 (Kiuchi in view of Pfaffenberger and Rivest) Dependent Claim 7 (Kiuchi in view of Pfaffenberger and Borella) Dependent Claims 20, 21, 35, 44 and 45 (Kiuchi in view of Pfaffenberger and Broadhurst) Dependent Claims 31, 33, 35 and 56 (Kiuchi in view of Pfaffenberger and Ludwig)

The patent owner sets forth arguments (Response at 32 & 33) previously addressed above.

3.7. Secondary Considerations of Non-obviousness

The patent owner has not established a *nexus* between the secondary evidence and the claimed invention. MPEP 716.01.b. The patent owner argues there is substantial evidence of secondary considerations to demonstrate nonobviousness regarding claims 1-60, but fails to describe how the evidence specifically relates to the subject matter of any of the claims. (Response at 44 & 45). The Declaration by Robert Dunham Short III, filed with the Response, (the "Short Declaration") mentions some of the limitations in claims 1, 8, 9, 16 and 27, but then asserts the long-felt need was for a "system that could be easily and correctly used to enable secure communications." Paragraph 3. It is not clear how this highly generalized need specifically relate to the limitations of the mentioned claims (*nexus*), moreover nothing is stated about the remaining claims 2-7, 10-15, 17-26 and 28-60. For example, no claims recite the user "easily" and "correctly" enabling secure communications.

As noted by the requester (Comment at 31), the alleged need for a "system that could be easily and correctly used to enable secure communications" is such a broad need that the patent

owner has not demonstrated whether the prior art, such as Lendenmann, Aziz, Kiuchi and Pfaffenberger, satisfied this need. If limitations such as "an indication that the domain name service system supports establishing a secure communication link" identified by the patent owner allow the user to in some unspecified manner to "easily" and "correctly" enable secure communications, then it would seem various prior art DNS security feature in the applied prior art would also allow the user to "easily" and "correctly" enable secure communications in a same, similar or different manner. The long-felt need must not have been satisfied by another before the invention by patent owner. MPEP 716.04.II.

The patent owner alleges commercial success, but attributes the commercial success to the licensing of a patent family not specifically identifying any claim in the subject patent under reexamination. Short Declaration, paragraph 12. Thus, the patent owner has not provided established a *nexus* between the evidence of commercial success and the claims of the patent under reexamination.

Similarly, the patent owner alleges the skepticism of experts and praise, but identifies no claims describing subject matter of which the experts were skeptical or for which praise was given. Short Declaration, paragraphs 13-16. Thus, the patent owner has not provided established a *nexus* between the evidence of commercial success and the claims of the patent under reexamination.

The examiner also notes the declarant was Robert Short, who is the patent owner's Chief Technology Officer, thus raising a question as to whether the declaration was self-interested thereby according less weight.

4. Final Decisions Favorable to Patentability

4.1. The Rejection of Claim 11 As Obvious Over Lendenmann in View of Martin Is Withdrawn

The patent owner is correct that the incorporated 103 rejection over Lendenmann in view of Martin is deficient for failing to teach an "network address hopping regime that is used to pseudo randomly change network addresses in packets transmitted…." See the earlier Response, filed June 3, 2012, pp. 24 & 25. While the requester asserts the Martin secondary reference teaches changing the source address in the packets transmitted, the incorporated rejection does not address how this change implements a network address "hopping" regime. The term "network address *hopping* regime" cannot be meaningfully interpreted without referring to the specification, which discloses a communicating pair of nodes *hopping* to mutually agreed-upon source and destination addresses selected from a block of IP addresses using an algorithm and a randomization seed. *See* Larson, col. 39, ll. 36-40, which refers back to previous discussions of address hopping. One such discussion extensively occurs at col. 17, ll. 1-16.

4.2 The Rejection of Claims 11-13 As Obvious Over Aziz in View of Martin Is Withdrawn

The patent owner is correct that the incorporated 103 rejection over Aziz in view of Martin is deficient for failing to teach an "network address hopping regime that is used to pseudo randomly change network addresses in packets transmitted…." (claim 11) and "comparing a value in each data packet transmitted...." (claim 12). Response, pp. 48-50. While the requester asserts the Martin secondary reference teaches changing the source address in the packets transmitted, the incorporated rejection does not address how this change implements a network address "hopping" regime. The term "network address *hopping* regime" cannot be meaningfully interpreted without referring to the specification, which discloses a communicating pair of nodes *hopping* to mutually agreed-upon source and destination addresses selected from a block of IP addresses using an algorithm and a randomization seed. *See* Larson, col. 39, ll. 36-40, which refers back to previous discussions of address hopping. One such discussion extensively occurs at col. 17, ll. 1-16. Regarding claims 12 and 13, the incorporated rejection admits that neither Aziz or Martin teach comparing the source of the data packets ("value in each data packet") as coming from one of the range of valid values recited in the claims ("moving window of valid values") or comparing a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for a first device. See, e.g., pages 99 and 100 of the incorporated claim chart attached as Exhibit F-2 to the Request.

4.3. The Rejection of Claim 11 As Obvious Over Kiuchi in View of Pfaffenberger and Martin Is Withdrawn

The patent owner is correct that the incorporated 103 rejection over Kiuchi in view of Pfaffenberger and Martin is deficient for failing to teach an "network address hopping regime

that is used to pseudo randomly change network addresses in packets transmitted…." (claim 11). While the requester asserts the Martin secondary reference teaches changing the source address in the packets transmitted, the incorporated rejection does not address how this change implements a network address "hopping" regime. The term "network address *hopping* regime" cannot be meaningfully interpreted without referring to the specification, which discloses a communicating pair of nodes *hopping* to mutually agreed-upon source and destination addresses selected from a block of IP addresses using an algorithm and a randomization seed. *See* Larson, col. 39, ll. 36-40, which refers back to previous discussions of address hopping. One such discussion extensively occurs at col. 17, ll. 1-6.

5. Conclusion

This is a RIGHT OF APPEAL NOTICE (RAN); see MPEP § 2673.02 and § 2674. The decision in this Office action as to the patentability or unpatentability of any original patent claim, any proposed amended claim and any new claim in this proceeding is a FINAL DECISION.

No amendment can be made in response to the Right of Appeal Notice in an *inter partes* reexamination. 37 CFR 1.953(c). Further, no affidavit or other evidence can be submitted in an *inter partes* reexamination proceeding after the right of appeal notice, except as provided in 37 CFR 1.981 or as permitted by 37 CFR 41.77(b)(1). 37 CFR 1.116(f).

Each party has a **thirty-day or one-month time period, whichever is longer**, to file a notice of appeal. The patent owner may appeal to the Board of Patent Appeals and Interferences

with respect to any decision adverse to the patentability of any original or proposed amended or new claim of the patent by filing a notice of appeal and paying the fee set forth in 37 CFR 41.20(b)(1). The third party requester may appeal to the Board of Patent Appeals and Interferences with respect to any decision favorable to the patentability of any original or proposed amended or new claim of the patent by filing a notice of appeal and paying the fee set forth in 37 CFR 41.20(b)(1).

In addition, a patent owner who has not filed a notice of appeal may file a notice of cross appeal within **fourteen days of service** of a third party requester's timely filed notice of appeal and pay the fee set forth in 37 CFR 41.20(b)(1). A third party requester who has not filed a notice of appeal may file **a notice of cross appeal within fourteen days of service** of a patent owner's timely filed notice of appeal and pay the fee set forth in 37 CFR 41.20(b)(1).

Any appeal in this proceeding must identify the claim(s) appealed, and must be signed by the patent owner (for a patent owner appeal) or the third party requester (for a third party requester appeal), or their duly authorized attorney or agent.

Any party that does not file a timely notice of appeal or a timely notice of cross appeal will lose the right to appeal from any decision adverse to that party, but will not lose the right to file a respondent brief and fee where it is appropriate for that party to do so. If no party files a timely appeal, the reexamination prosecution will be terminated, and the Director will proceed to issue and publish a certificate under 37 CFR 1.997 in accordance with this Office action.

The Patent Owner is reminded of the continuing responsibility under 37 CFR 1.985(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the subject Alden patent throughout the course of this reexamination proceeding. The Third Party Requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding through the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

All correspondence relating to this *inter partes* reexamination proceeding should be directed as follows:

By **U.S. Postal Service Mail** to:

Mail Stop *Inter Partes* Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand to: Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Roland G. Foster/
Roland G. Foster
Primary Examiner
Central Reexamination Unit 3992

Conferee:
/BJP/

Conferee:
/Daniel J Ryman/
Supervisory Patent Examiner, Art Unit 3992