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.
95/001,789	10/18/2011	7921211	41484-80150	6053

22852 7590 06/26/2013

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
06/26/2013	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	
	95/001,789	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)

SIDLEY AUSTIN LLP
717 NORTH HARWOOD
SUITE 3400
DALLAS, TX 75201

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
	95/001,789	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 26 December, 2012
Third Party(ies) on 23 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 _____ are patentable. [Amended or new claims].
5. ☒ Claims 1-60 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. ☐ _____

RIGHT OF APPEAL NOTICE

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 January 18, 2012 in response to a Request for *Inter Partes* Reexamination, filed October 18, 2011 (the "Request").

An Action Closing Prosecution ("ACP") mailed September 26, 2012 rejected all original claims 1-60 of the Larson patent.

The patent owner responded by filing arguments and associated evidence on December 26, 2012 (the "Response").

The third party requester responded by filing Comments on the Patent Owner's Response on January 23, 2013 (the "Comments").

Evidence Submitted After the ACP

The patent owner submitted the Supplemental Declaration of Angelos D. Keromytis, Ph.D. on December 26, 2012 (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)

There are no final decisions favorable to patentability.

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

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

Solana, E. et al., "Flexible Internet Secure Transactions Based on Collaborative Domains," Lecture Notes in Computer Science, Vol. 1361, at 37-51 (1997), attached to the Request as Exhibit X1 ("Solana").

U.S. Patent No. 6,557,037 to Provino, attached to the Request as Exhibit X2 ("Provino").

U.S. Patent No. 6,496,867 to Beser, attached to the Request as Exhibit X3 ("Beser").

Atkinson, R., IETF RFC 2230, "Key Exchange Delegation Record for the DNS," November 1997, attached to the Request as Exhibit X4 ("RFC 2230").

Eastlake, D. et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)," March 1999, attached to the Request as Exhibit X5 ("RFC 2538").

Kent, S. et al., IETF RFC 2401, "Security Architecture for the Internet Protocol," November 1998, attached to the Request as Exhibit X6 ("RFC 2401").

Eastlake, D. et al., IETF RFC 2064, "Domain Name System Security Extensions," January 1997, attached to the Request as Exhibit X7 ("RFC 2065").

Postel, J. et al., IETF RFC 920, "Domain Requirements," October 1984, attached to the Request as Exhibit X8 ("RFC 920").

Guttman, E. et al., IETF RFC 2504, "Users' Security Handbook," February 1999, attached to the Request as Exhibit X9 ("RFC 2504").

Reed, M. et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, Sand Diego, CA (December 9-13, 1996), attached to the Request as Exhibit X10 ("Reed").

The third party requester also cited six prior art patents and printed publications to demonstrate the knowledge in the field of the invention.

Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK, May 1996, attached to the Request as Exhibit Y1 ("Goldschlag").

Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987, attached to the Request as Exhibit Y2 ("RFC 1035").

Braken, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989, attached to the Request as Exhibit Y3 ("RFC 1123").

Atkinson, R., RFC 1825, "Security Architecture for the Internet Protocol," August 1995, attached to the Request as Exhibit Y4 ("RFC 1825").

Housley, R. et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL profile," January 1999, attached to the Request as Exhibit Y5 ("RFC 2459").

Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987, attached to the Request as Exhibit Y4 ("RFC 1034").

2.D. Summary Regarding Those Proposed Rejections Adopted by the Examiner

The rejections identified in Issues 1-35 are adopted because the stated combinations establish a reasonable likelihood that the requester will prevail with respect to at least one of the claims 1-60 in the Larson patent, as explained in said Order.

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

Some of the references cited are intervening art. MPEP 2617. Requestor asserts that the instant claims are not entitled to the earliest filing date of June 7, 1998, the filing date of the oldest parent, provisional application. The examiner agrees. U.S. Patent No. 7,010,604, which issued from parent application 09/429,643, and which was filed Oct. 29, 1999, fails to explicitly recite nor imply the phrase "domain name service" present in all independent claims in the Larson patent for which reexamination is now sought. Indeed, the 7,010,604 patent does not appear to even be directed to services similar to domain name lookup. The patent thus fails to neither provide written description support nor enable the subject matter recited in claims 1-60 of the Larson patent. Accordingly, the Larson patent is not entitled to the benefit of the 7,010,604 patent filing date. The effective filing date for claims 1-60 is no earlier than the Feb. 15, 2000 filing date of the U.S. Patent No. 6,502,135, which issued from parent application 09/504,783.

2.F. Rejections Based upon Solana (Issues 1-8)

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.

Claims 1, 2, 5, 6, 8, 9, and 14-60 are rejected under 35 U.S.C. 102(b) as being anticipated by Solana.

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 though 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.

Claims 2-5, 24, 25, 37, 48, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of RFC 920.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of Reed.

Claims 7, 32 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of Beser.

Claims 1, 2, 5, 6, 8, 9 and 14-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504.

Claims 2-5, 24, 25, 37, 48 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504, and further in view of RFC 920.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504, and further in view of Reed.

Claims 7, 32 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504, and further in view of Beser.

Incorporation by Reference

Thus, the third party requester proposed rejection of claims 1-60 on pages 14-117 of the Request and Exhibits C1 and C2 (claim charts), are adopted and incorporated by reference.

2.G. Rejections Based upon Provino (Issues 9-20)

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 –
>
> (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.

Claims 1, 2, 5, 6, 8, 9 and 14-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Provino.

Claim Rejections - 35 USC § 103

Claims 2-5, 24, 25, 37, 48, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 920.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of Reed.

Claims 7, 29-32 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solana as applied to the respective, parent claims above (if applicable), and further in view of Beser.

Claims 1, 2, 5, 6, 8, 9 and 14-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 2230.

Claims 2-5, 24, 25, 37, 48 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 2230, and further in view of RFC 920.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further view of RFC 2230, and further in view of Reed.

Claims 7, 29-32 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 2230, and further in view of Beser.

Claims 1, 2, 5, 6, 8, 9 and 14-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504.

Claims 2-5, 24, 25, 37, 48 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504, and further in view of RFC 920.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further view of RFC 2504, and further in view of Reed.

Claims 7, 29-32 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Provino as applied to the respective, parent claims above (if applicable), and further in view of RFC 2504, and further in view of Beser.

Incorporation by Reference

Thus, the third party requester proposed rejection of claims 1-60 on pages 118-225 of the Request and Exhibits C3, C4 and C5 (claim charts), are adopted and incorporated by reference.

2.H. Rejections Based upon Beser (Issues 21-24)

Claim Rejections - 35 USC § 102

Claims 1, 2, 5-7 and 14-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Beser.

Claim Rejections - 35 USC § 103

Claims 2-5, 24, 25, 37, 48, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beser as applied to the respective, parent claims above (if applicable), and further in view of RFC 920.

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beser as applied to the respective, parent claims above (if applicable), and further in view of RFC 2401.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beser as applied to the respective, parent claims above (if applicable), and further view of RFC 2401, and further in view of Reed.

Incorporation by Reference

Thus, the third party requester proposed rejection of claims 1-60 on pages 226-277 of the Request and Exhibit C6 (claim chart), are adopted and incorporated by reference.

2.I. Rejections Based upon RFC 2230 (Issues 25-29)

Claim Rejections - 35 USC § 102

Claims 1, 2, 6, 7 and 14-60 are rejected under 35 U.S.C. 102(b) as being anticipated by RFC 2230.

Claim Rejections - 35 USC § 103

Claims 2-5, 24, 25, 37, 48, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2230 as applied to the respective, parent claims above (if applicable), and further in view of RFC 920.

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2230 as applied to the respective, parent claims above (if applicable), and further in view of RFC 2401.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2230 as applied to the respective, parent claims above (if applicable), and further view of RFC 2401, and further in view of Reed.

Claims 29-32 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2230 as applied to the respective, parent claims above (if applicable), and further in view of RFC 2230, and further in view of Beser.

Incorporation by Reference

Thus, the third party requester proposed rejection of claims 1-60 on pages 278-323 of the Request and Exhibit C7 (claim chart), are adopted and incorporated by reference.

2.J. Rejections Based upon RFC 2538 (Issues 30-35)

Claim Rejections - 35 USC § 102

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1, 2, 6, 14-22, 24-46, 48-52 and 57-60 are rejected under 35 U.S.C. 102(a) as being anticipated by RFC 2538.

Claim Rejections - 35 USC § 103

Claims 3, 4, 24, 25, 48 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2538 as applied to the respective, parent claims above (if applicable), and further in view of RFC 920.

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2538 as applied to the respective, parent claims above (if applicable), and further in view of RFC 2401.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2538 as applied to the respective, parent claims above (if applicable), and further view of RFC 2401, and further in view of Reed.

Claims 7, 29-32 and 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2538 as applied to the respective, parent claims above (if applicable), and further in view of Beser.

Claims 5, 23 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2538 as applied to the respective, parent claims above (if applicable), and further in view of RFC 2065.

Incorporation by Reference

Thus, the third party requester proposed rejection of claims 1-60 on pages 324-366 of the Request and Exhibit C8 (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. 35-48, 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, June 25, 2012, ¶ 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 with the Response (the original "Keromytis" declaration), ¶ 17-19.

Regarding whether the DNS device(s) are a separate device, 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. 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* the original Keromytis Declaration, ¶ 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.

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.....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 Larson patent's description of gatekeeper 2603, DNS proxy 2610, and DNS server 2609 to support its unreasonable interpretation of a

DNS system. However, the Larson patent discloses significant DNS functionality and coordination between these devices in acting upon a DNS request." (Response at 3, 4) (*See also* said original Keromytis Declaration, ¶¶ 17-19).

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 Larson 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 Larson 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 the "SDNS only returns a secure URL after it has already coordinates with the VPN gatekeeper to establish a VPN." (Respond at 7). Then, "in step 3410, the SDNS 3313 returns a secure URL either through an administrative VPN link or 'in the clear,' it does not matter which." (*Id.*)

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 51:37-50) (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.

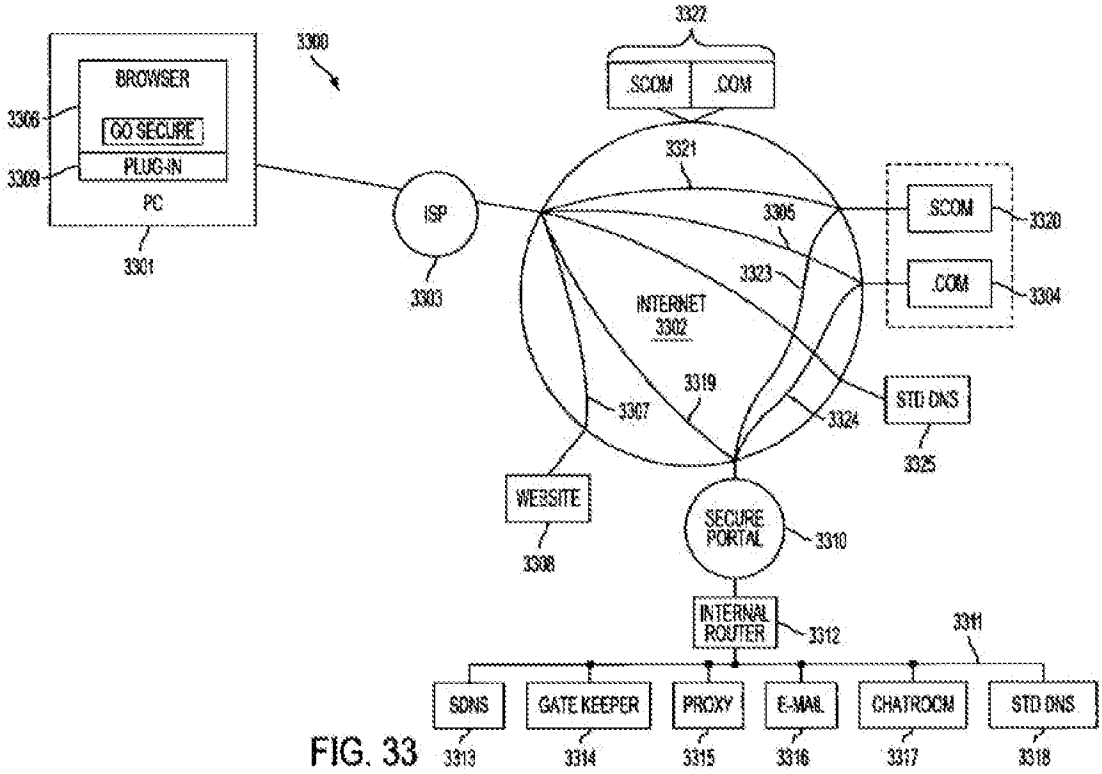
3300
BROWSER
GO SECURE
PLUG-IN
PC
3301
3306
3309
ISP
3303
3322
.SCOM
.COM
3321
3305
3323
INTERNET
3302
3307
3319
3324
SCOM
3320
.COM
3304
STD DNS
3325
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
SDNS
3313
GATE KEEPER
3314
PROXY
3315
E-MAIL
3316
CHATROOM
3317
STD DNS
3318

FIG. 33

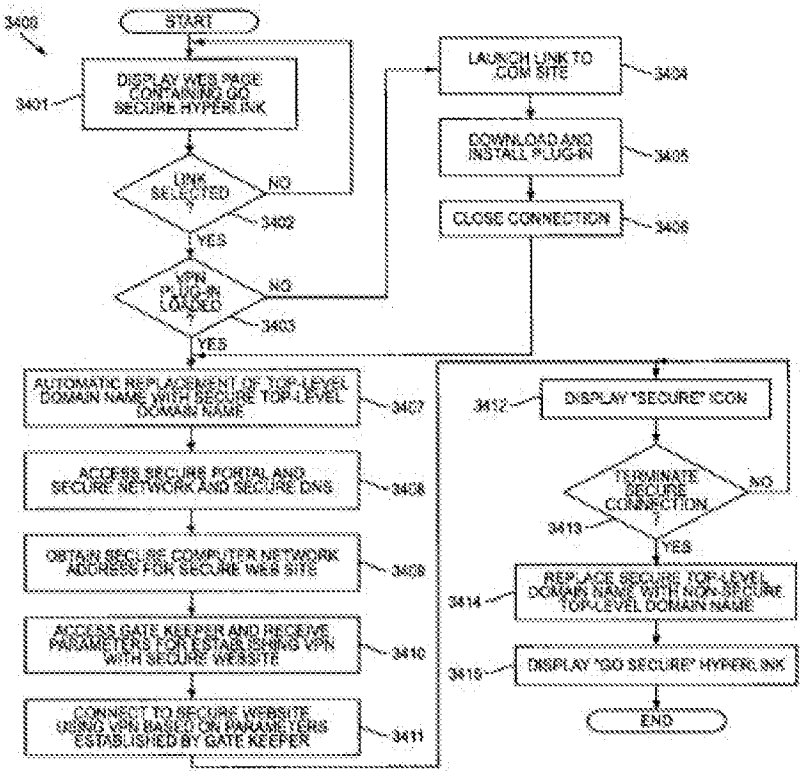
3400
START
3401
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
LINK SELECTED
NO
3402
YES
VPN PLUG-IN LOADED
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE 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 AND ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION
NO
3413
YES
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. 22-35) 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 Solana's use of certificates and encryption keys discloses the recited indication, without explaining how the user of certificates and keys provides a 'visible message or signal to a user....In fact, those skilled in the art would have understood that certificates and encryption keys were *not 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). 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. 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). 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 "support" 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. The original Declaration of Angelos D. Keromytis, PhD., ¶ 17-19, filed on April 18, 2012 in this proceeding. 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 Keromytis Declaration, ¶ 18.

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 regarding 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 indications that it will do so, such as providing cryptographic services (Solana), establishing a VPN (Provino), providing a secure address to the user (Besser), providing key exchanger services (RFC 2230), and security certificates (RFC 2538).

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 6). "Never does the specification equate the mere return of requested DNS records, such as an IP address or key certificate, 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. As the requester notes, 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…." (Comments at 4). 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 Solana

3.3.A Background

Solana teaches a "Directory Service (DS) holding naming information....As mentioned, existing naming infrastructures (DNS-sec, X.509) might be used for this purpose." P.43. Solana cites to RFC 2065 as an example of said DNS-sec (reference 16). RFC 2065 (DNS

Security Extensions), as the name suggests, is an extension to DNS and thus cites to and incorporates RFC 1033, 1034 and 1035, which describe the conventional naming infrastructure of DNS. RFC 2065, abstract and section 1. Thus, the DNS-sec embodiment of Solana incorporates at least RFC(s) 1034, 1035 and 2065. RFC(s) 1034, 1035 and 2065 are also of record in this proceeding. The naming information in DNS, as is notoriously well known by one of ordinary skill, includes domain names and their corresponding addresses. *See, e.g.*, RFC 1034, section 3.6. *See also* the requester's Fratto Declaration, ¶ 34.

Solana teaches at p. 43 (emphasis added):

> A coordinated global ***Directory Service*** (DS) holding **naming information and** especially **certificates that securely bind domains to their public keys** is also required and constitutes the cryptographic support for inter-domain transactions. As mentioned, existing naming infrastructures (**DNS-sec**, X.509) **might be used for this purpose**.
>
> A well-defined convention establishing an ***Uniform Naming Information*** (UNI) is also needed to **designate principals and domains globally and unequivocally** as, for instance, a common name, an E-mail address, or a **network address**. Note that **this information** may also be **published** in the Directory Service.
>
> The information necessary for the provision of secure end-to-end transactions is kept in the ***Local Authentication Database*** (LAD) that will **contain for each principal (UNI) the local authentication credentials**: for this, we propose to use an asymmetric cryptosystem with the principal owning the private key and the LAD holding the corresponding public key[].

Thus, Solana teaches of a DNS system that stores both "naming information" and certificate information. The certificates bind "domains to their public keys" by using globally unique, identifying information (UNIs) about the owner of the public key. The UNI includes a network address, which is published in the local authentication database (LAD). One of ordinary skill would certainly understand that information is "published" in the LAD for the purpose of

reading by the public (searching). Thus, Solana at the least teaches the DNS system is queried using a UNI network address in order to retrieve the corresponding public key.

Solana however further teaches the DNS system stores a plurality of domain names and network addresses, where a query containing a domain name is used to retrieve a network address and the corresponding public key (if it exists). Specifically, the Solana teaches that the DNS system, in one embodiment, uses DNS-sec as described in RFC 2065 and in turn RFC(s) 1033, 1034 and 1035, as discussed above. RFC 1034 teaches that a type "A" (containing the IP address) resource record ("RR") is sent in response to a standard query specifying a domain name. Sections 3.6, 3.7, 3.7.1. RFC 2065 teaches that the public key "must be included if space is available" in a type "A" (host address) RR (section 3.7), which as just discussed, is sent in response to a standard query specifying a domain name. Thus, the Solana DNS-sec embodiment teaches the DNS system that stores domain name and corresponding network address information.

A conventional DNS query specifying a domain name returns both the IP address and a public key in a type "A" RR if (1) space is available in the type "A" RR; and if (2) the retrieved network address matches a UNI (e.g., network address) corresponding to a public key. *See also* the Fratto declaration, ¶s 39-45.

3.3.B. Claims 1, 36 and 60

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

The third party requester repeatedly references statements made before a district court in a related proceeding regarding claim interpretation (e.g., Comments at 7), but fails to provide the examiner with even a date (as indicated in public PAIR) when this evidence was filed of record with the Office. The examiner has searched the extensive record in this case without the aid of a locating filing date, but was unable to find any of the cited statements.

The patent owner maintains Solana does not incorporate RFC 2065. Instead, Solana merely references this RFC and does not "identify" with detailed particularity what specific material it incorporates and where the material is found. Moreover, it is argued, Solana does not even mention RFCs 1034 and 1035. (Response at 11).

The examiner does not agree. Solana teaches a "Directory Service (DS) holding naming information....As mentioned, existing naming infrastructures (DNS-sec, X.509) might be used for this purpose." (P.43). Solana cites to RFC 2065 as an example of said DNS-sec (reference 16). RFC 2065 (DNS Security Extensions), as the name suggests, is an extension to DNS and thus cites to and incorporates RFC 1033, 1034 and 1035, which describe the conventional naming infrastructure of DNS. RFC 2065, abstract and section 1. RFC(s) are among the most

authoritative publications for Internet systems and protocols. One of ordinary skill in the art of Internet based communications would be quite familiar with technical documents citing to RFC(s) and would have understood that, if not indicated otherwise, the entire RFC was being incorporated because it typically teaches implementing specific protocol functions in a standardized manner. Moreover, if the incorporated RFC relies upon underlying RFCs (e.g., the DNS-sec protocol described in RFC 2065 relies upon common DNS protocol elements described in RFC 1033, 1034 and 135), then those RFC are incorporated too, otherwise RFC 2065 would be inoperative and incomplete to one of ordinary skill. The patent owner urges the examiner to rely on an "incorporation by reference" scheme at odds with how one of ordinary skill in the art would interpret the citation of RFC(s) in the field of Internet communications. *See also* the requester's comments. (Comments at 9 & 10).

The patent owner also asserts that even if Solana incorporates RFC 2065 to hold naming information and certificates, Solana still fails to teach "storing domain names and corresponding network addresses or receiving a query for a network address." (Response at 11 & 12).

The examiner does not agree. Solana teaches that the DNS system, in one embodiment, uses DNS-sec as described in RFC 2065 and in turn RFC(s) 1033, 1034 and 1035, as discussed above. RFC 1034 teaches that a type "A" (containing the IP address) resource record ("RR") is sent in response to a standard query specifying a domain name. (Sections 3.6, 3.7, 3.7.1). RFC 2065 teaches that the public key "must be included if space is available" in a type "A" (host address) RR (section 3.7), which as just discussed, is sent in response to a standard query

specifying a domain name. Thus, the Solana DNS-sec embodiment teaches the DNS system that stores domain name and corresponding network address information. A conventional DNS query specifying a domain name returns both the IP address and a public key if (1) space is available in the type "A" RR; and if (2) the retrieved network address matches a UNI (e.g., network address) corresponding to a public key. See also the Fratto declaration, ¶s 39-45. *See also* the requester's remarks regarding this issue. (Comment at 10 & 11).

3.3.C Claims 5, 23 and 47

The patent owner argues Solana fails to disclose a "domain name service system…configured to authenticate the query…." (Response at 12). Solana however explicitly teaches authentication of the query and a relationship between authentication and encryption parameters. *See e.g.*, p. 43 (emphasis added):

> The information necessary for the provision of secure end-to-end transactions is kept in the ***Local Authentication Database*** (LAD) that will contain for each principal (UNI) the **local authentication credentials**: for this, we propose to use an asymmetric cryptosystem with the principal owning the private key and the LAD holding the corresponding public key[].

See also the requester's remarks regarding this issue. (Comments at 12 & 13).

3.3.D. Claims 8 and 9

The patent owner asserts Solana fails to teach that "the domain name service system is connectable to a virtual private network through the communication network." (Response at 14).

Solana however teaches "organizations concerned by security issues…interact with the Internet…by means of well-protected *Virtual Private Networks* (VPN)," which is not a suggestion. P. 38. Moreover, VPN(s) are established between VPN-capable hosts (e.g., VPN capable routers or servers) using the IP security protocol (Ipsec) and only rely upon conventional DNS capability. *See, e.g.*, RFC 2401, of record in this proceeding. As discussed in section 3.3.A above, the Solana DNS-sec embodiment relies upon the underlying infrastructure of a conventional DNS, which therefore supports the establishment of VPN(s).

3.3.E. Claims 18 and 42

The patent owner incorrectly asserts that the UNI is not reserved for secure communications links. (Response at 15). The claim recites "at least one of the plurality of domain names is reserved for secure communication links." As explained in section 3.3.A above, the Solana DNS-sec embodiment teaches the DNS system that stores domain name and corresponding network address information. A conventional DNS query specifying a domain name retrieves both the network address and a public key if (1) space is available in the type "A" RR; and if (2) the retrieved network address matches a UNI (e.g., network address) corresponding to a public key. In such a case, the domain name is reserved for secure communication links although certainly the initiator is not required to then establish a secure communication link (i.e., take advantage of the reservation). For example, the type "A" RR may not have space available or the retrieved network addressed may not match the UNI (network address) corresponding to the public key. Regardless, the domain name is still reserved

for eventual secure communications, such as when there is room in the type A RR and when retrieved address matches the UNI.

3.3.F. Claims 24 and 48

The patent owner argues Solana 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 15 and 16).

The requester responds that the first Office action determined Solana taught a functional relationship between a secure domain name associated with the certificate and establishing a secure communication to that domain. The patent responded by asserting the domain name itself comprised the indication and thus it was the name that distinguished over the prior art. In the current response, the patent owner now asserts a functional relationship between the domain names and the DNS. (Comments at 15).

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, Solana teaches such a system.

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. 13-23) 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.

3.3.G. Remaining Arguments Regarding Solana

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

3.4. Response to Patent Owner and Third Party Requester Comments Regarding Solana in view of Reed

3.4.A. Claim 10

The patent owner argues Reed fails to teach pseudo randomly changing IP addresses because it routes the IP traffic according to pre-defined schemes. (Response at 18 & 19, citing back to the Response to the non-final Office action). The incorporated rejection however cited to Goldschlag to demonstrate knowledge in the field of the invention that onion routing involves "loose routing," where "[i]t is not necessary that the entire route be prespecified by the iniator's proxy." (Request at 86, foot note 4) (*See also* Goldschlag at 6). The patent owner has not addressed Goldschlag or whether knowledge in the field of the invention included the knowledge that onion routing involves loose (pseudorandom) routing.

3.4.B. Claim 12

The patent owner asserts Reed fails to teach "the virtual private network is based on comparing a value in each data packet transmitted between a first device and a second device to a moving window of said values." The patent owner acknowledges "Reed teaches that '[w]hen a data cell arrives, the onion router looks up the cell's identifier in its tables and finds the corresponding outbound identifier." The patent owner however argues "Reed does not disclose that these identifiers in the table are including in a moving window of valid values or comparing those identifiers to such a moving window...." (Response to the non-final Office action at 47 & 48). As discussed above regarding claim 10 however, onion routing involves loose

(pseudorandom) routing and thus the window would move in accordance with unspecified pseudorandom identifiers making up the route.

3.5. Response to Patent Owner and Third Party Requester Comments Regarding Provino

3.5.A. Background

Provino's teachings share substantial, structural similarity with an embodiment of the patent under reexamination. For example, the Larson patent under reexamination discloses an embodiment at col. 40, l. 66 – col. 41, l. 16:

> Some or all of the security functions can be embedded in gatekeeper 2603, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy 2610 communicates with gatekeeper 2603 to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:
>
> (210) Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

Thus in the Larson patent under reexamination, the DNS proxy 2610 receives a DNS request from the client (initiator) and then forwards it to gatekeeper 2603. The gatekeeper 2603 is also part of the DNS system because it processes the DNS request. The gatekeeper 2603 then establishes a VPN connection with the query initiator (client). The establishment of a VPN

connection between the client and gatekeeper 2603 is an "indication that the domain service name service system supports establishing a secure communication link."

Similarly, the Provino prior art teaches that name server 17 receives DNS request (query by domain name) from device 12(m) (initiator) and responds by providing the corresponding Internet address, which in one embodiment is the address of firewall 30. Col. 7, ll. 36-41 and col. 9, ll. 46-57. A secure tunnel connection (VPN) between the firewall 30 and the query initiator device 12(m) is then established. The firewall 30 is also part of the DNS system because it independently provides device 12(m) with the identification of VPN nameserver 32 (col. 10, ll. 63-67, col. 12, ll. 37-61). The firewall 30 then receives a name request from device 12(m), decrypts and analyzes this request, then transmits a modified name request to VPN server 32 (col. 14, ll. 1-38). The VPN Name Server 32 provides the requested network address to in a message packet to the firewall 30, where the firewall then transmits the address to device 12(m) encrypted within a secure VPN tunnel. Thus, firewall 30 forms a functional and structural part of a distributed DNS system consistent with the specification of the patent under reexamination. See section 3.1 above. The establishment of a secure connection between the query initiator (device 12(m)) and firewall 30 is an indication that the DNS "supports establishing a secure communication link." An indication is also provided when firewall 30 provides device 12(m) with the identification of VPN name server 32 within VPN 15 (secured network) as well as when firewall 30 provides device 12(m) with the Internet address of a secure server 31 within VPN 15. Col. 10, l. 56 - col. 11, l. 25. Regardless, the indication is provided by a DNS system (e.g., DNS name server 17, firewall 30, VPN server 32) and not just name server 17.

Even if name server 17, when considered in isolation, provides an "indication" as claimed. As discussed, name server 17 answers the name query by providing a network address that is not the actual address of the destination computer. Similarly, in one embodiment the patent owner's DNS proxy 2610 answers a query by "preferably using a secure administrative VPN." Larson, col. 40, ll. 3-8. 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. 37-50, 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. Just as the eventual establishment of a VPN between the user computer and secure target site in Larson provides the "indication," Provino also teaches the eventual establishment of a VPN between user device 12(M) and secure server 31. Thus, even the name server 17, when considered by itself, provides the "indication" as broadly claimed and consistent with the specification of the patent under reexamination. *See also* Section 3.2.B above for additional discussion regarding the recited term "indication."

The biggest difference between the Larson and Provino teachings discussed above is that, in Larson, the DNS proxy 2610 forwards the message to gatekeeper 2603 while, in Provino, the DNS server 17 provides a network address that the initiator uses to contact firewall 30. However, whether the DNS request is forwarded or redirected is an unclaimed feature not necessary for an understanding of the claims.

3.5.B. Claim 1

The patent owner asserts firewall 30 is not part of the DNS system because it has no DNS-related functionality. "Rather, the role of Provino's firewall 30 is limited to a few typical firewalling functions for 'control[ling] access by devices external to the virtual private network 15 to servers 31(s) within the virtual private network 15'" (Response at 22).

The patent owner however has just described an embodiment disclosed in their own specification. As discussed in section 3.2.A. regarding 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.*). Thus, the firewall 30 in Provino, which provides access control to a DNS server behind the firewall, can be considered part of the DNS system just as the secure portal 3312, which provides access control to a DNS server behind the portal, is considered part of the DNS system in the patent owner's specification (especially regarding the embodiment of col. 51, ll. 37-50).

The firewall 30 is also part of the DNS system for additional reasons. The firewall 30 independently provides device 12(m) with the identification of VPN nameserver 32 (col. 10, ll. 63-67, col. 12, ll. 37-61). The firewall 30 then receives a name request from device 12(m), decrypts and analyzes this request, then transmits a modified name request to VPN server 32

(col. 14, ll. 1-38). Moreover, as the requester notes, the VPN Name Server 32 provides the requested network address to in a message packet to the firewall 30, where the firewall then transmits the address to device 12(m) encrypted within a secure VPN tunnel. (Comments at 21). Thus, firewall 30 forms a functional and structural part of a distributed DNS system consistent with the specification of the patent under reexamination.

The patent owner argues the establishment of a secure tunnel between the external device 12(m) and firewall 30 is not "an indication that the domain name service system supports establishing a secure communication link." (Response at 26 & 27). This assertion is first based on the examiner's claim construction being unreasonably broad, but the examiner disagrees for the reasons previously discussed in section 3.1. The patent owner also bases the assertion on the establishment of secure tunnel failing to provide a visible message or signal to a user, but such an establishment would provide a signal to the user as discussed in Section 3.2.B. Finally, the patent owner urges the "establishment of the secure tunnel in Provino is also itself an 'indication' is contrary to the language of claim 1. Claim 1 makes clear the 'indication' and the 'establishing' are two separate elements…." The patent owner's arguments are premised on the "indication" happening at a different time than the "establishing." A plain English reading of the limitation imposes no such requirement. "Establishing a secure communication link" is not a future tense expression. Rather, it appears to be present tense and thus denotes what is happening approximately now. Thus, an "indication" and "supports establishing a secure communication link" may happen at approximately the same time. Not surprisingly then, the language embraces embodiments disclosed in the patent owner's specification, such as the

embodiment of col. 48, ll. 60-66 (VPN upon boot up) and col. 51, ll. 37-50 (VPN established after query and response in the clear) where the indication is provided at approximately the same time that the VPN is established.

The patent owner asserts providing the device 12(m) with the address of the VPN name server 32 is not an "indication that the domain name service system supports establishing a secure communication link." (Response at 27 & 28). As discussed in section 3.2.B however, the Larson patent discloses an embodiment 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 "indication" that the DNS in some manner supports establishing a communication link. In view of this, providing the user's computer with an identification of a VPN server certainly is part of the process of establishing a secure connection and thus is also indication that the DNS system will support secure communications. In another embodiment, the patent owner's DNS proxy 2610 answers a query by "preferably using a secure administrative VPN." (Larson, col. 40, ll. 3-8). 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. 3750 embodiment, where the secure DNS server 3313 receives and answers a query "in the clear" (*i.e.*, without using a VPN) from a

computer by providing the requested address. The computer then uses the address to establish a VPN link to the desired domain name.

The patent owner asserts that the name server 17 does not provide an indication that the DNS supports establishing a secure communication link when the server returns an address. (Response at 28 & 29). The examiner does not agree. Again, the patent owner discloses an embodiment at col. 51, ll. 37-50 where the DNS server provides an address to the requesting computer, which the computer then uses to establish a VPN with a secure domain.

3.5.C. Claims 5, 23 and 47

The patent owner argues authentication and authorization are not the same and rather have very specific meaning. Therefore, even though the examiner maintains the DNS system authenticates the query, that does not mean the same thing as authorize. (Response at 31 & 32). The examiner however agrees with the requester, who notes neither term is defined in the Larson specification to have a particular meaning nor would they have a precisely differ as alleged by the owner to one of ordinary skill in the art of Internet communications. (Comments at 25). Even assuming the owner's definitions to be true, Provino's authorization "verifies that the identity of the user has permission to access requested resources," and thus authenticates the user ("verifies the identity of a user") in relation to permission level.

The patent owner also alleges the examiner relied on different "queries," but as the requester notes, each query is part of the same sequence that results in establishment of the

secure connection. (Comment at 25). Moreover, as the requester notes, Provino teaches that, prior to querying the nameserver 32, firewall 30 (part of the DNS system) authorizes device 12(m) before a query is sent. *See* the Fratto Declaration, ¶ 56. *See also* Provino, col. 9, ll. 17-27 & 56-67, col. 12, ll. 56-59, and col. 13, ll. 8-15.

3.5.D. Claims 8 and 9

The patent owner's arguments (Response at 32 & 33) appear premised on the idea that name server 17 is the only part of Provino that belongs to a DNS system, which is incorrect for the reasons previously explained in section 3.1. The patent owner, in criticizing the teachings of Provino, instead describes an embodiment disclosed in their own specification. As discussed in Section 3.2.A regarding 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 computer then uses the address to establish a VPN link to the desired domain name. 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.*). Thus, the firewall 30 in Provino, which provides access control to a DNS server behind the firewall, can be considered part of the DNS system just as the secure portal 3312, which provides access control to a DNS server behind the portal, is considered part of the DNS system in the patent owner's specification (especially regarding the embodiment of col. 51, ll. 37-50).

3.5.E. Remaining Arguments Regarding Provino

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

3.6. Response to Patent Owner and Third Party Requester Comments Regarding Provino in view of RFC 920, Provino in view of Reed, Provino in view of Beser, Provino in view of RFC2230, Provino in view of RFC2230 and RFC 920, Provino and RFC 2230 in view of Reed, Provino and RFC 2230 in view of Beser, Provino in view of RFC 2504, Provino and RFC 2504 in view of RFC 920, Provino and RFC 2504 in view of Reed, Provino and RFC 2504 in view of Beser

The patent owner sets forth arguments (Response at 33-37) previously addressed above.

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

3.7.A. Claim 1

The patent owner argues *Beser* does not disclose a secure communication link and, thus, cannot disclose an indication that the domain name service system supports establishing a secure communication link. The patent owner alleges *Beser* teaches away from using encryption. (Response at 38 & 39). *See also* the original Keromytis Declaration, ¶ 58.

The patent owner misunderstands Beser. Rather than teaching away, Beser teaches its tunneling invention efficiently solves the problem of encrypted IP packets with readable source addresses. Thus, Beser must incorporate these encrypted packets otherwise Beser can't solve the

problem (readable source addresses) it explicitly discloses that it can. Specifically, Beser teaches "Of course, the sender may encrypt the information inside IP packets before transmission, e.g., with IP Security ("IPSec")." (Col. 1, ll. 54-56). Beser acknowledges IPSec "may require a great deal of computing power" that "may result in jitter, delay or loss of some packets" for streaming data flows, but states "Nonetheless, even if the information inside the IP packets could be concealed, the hacker is still capable of reading the source address of the packets." (Col. 2, ll. 1-5). Beser acknowledges various tunneling methods conceal the source address, but teaches the tunneling methods would require still more encryption or computational expense. (Col. 2, ll. 6-40). Beser thus teaches the solution is Beser's inventive tunneling method. (Col. 2, ll. 43-45). The solution involves hiding the source addresses in the packets and not all the information inside the IP packets (col. 3, ll. 4-9), which is not surprising because, as just discussed, Beser teaches that IPSec encrypted packets suffer from the problem of readable source addresses. Thus, Beser discloses a secure communication link.

Regardless, and contrary to the patent owner's assertions (Response at 39) nothing in the claim language requires the "secure communication link" to be encrypted. One of ordinary skill would understand this. For example, Beser teaches an unsecured Internet link can be secured by means other than encryption, such as hiding the source address so that the users cannot be mapped to a source address. (Beser, col. 1, ll. 26-53). Encryption is more secure than hiding the source address just as encryption and hiding the address is more secure than encryption only. The claims however do not recite the degree of security. *See also* the Fratto Declaration, ¶ 66. Thus, the patent owner's argument is directed to an unclaimed feature, which is unpersuasive.

The patent owner argues Beser only provides an address and thus fails to provide an "indication" of support for secure communication. (Response at 40 & 41). *See also* the original Keromytis Declaration, ¶ 60. The examiner does not agree.

First, as discussed in Section 3.2.B above, 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 court broadly construed the term to mean a visible message or signal to a user that the DNS system supports establishing a secure communication link. (*Markman* at 27). The examiner agrees.

Second, interpreting the claimed "indication" as a provision of an address is reasonably broad consistent with the specification. In the Beser prior art, a trusted DNS device provides a private address from a pool of private addresses in response to a query. Similarly, in one embodiment the patent owner's DNS proxy 2610 answers a query by merely providing a network address not necessarily (*i.e.*, "preferably") using a VPN. Larson, col. col. 40, ll. 3-8. *See also* col. 51, ll. 37-50, 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. Indeed, the private address from a pool of private addresses in Beser (col. 12, ll. 38-54) bears similarity to the "hop address" from a "hop block" disclosed in Larson (col. 17, ll. 1-38 and 39, ll. 35-40). The patent owner may argue that the eventual establishment of a VPN between the user computer and

secure target site in Larson provides the "indication," but as discussed above, Beser also teaches the eventual establishment of a secure communication (source address hidden). See also the Fratto Declaration, ¶ 60. Thus, Beser provides the "indication" as broadly claimed and consistent with the specification of the patent under reexamination.

3.7.B. Claims 18 and 42

The patent owner sets forth arguments (Response at 43) previously addressed above. The patent owner also asserts the Office improperly interprets the claim term "reserved," which is addressed in Section 3.3.E above.

3.7.C. Claims 24 and 48

The patent owner sets forth arguments (Response at 43 & 44) previously addressed above. The patent owner also asserts the Office improperly views the claims as directed to nonfunctional descriptive material, which is addressed in Section 3.3.F above.

3.7.D. Remaining Arguments Regarding Beser

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

3.8. Response to Patent Owner and Third Party Requester Comments Regarding Beser in view of RFC 920, Beser in view of RFC 2401, Beser in view of RFC 2401 and Reed

The patent owner sets forth arguments (Response at 45 & 46) previously addressed above.

3.9. Response to Patent Owner and Third Party Requester Comments Regarding RFC 2230

3.9.A. Claim 1

The patent owner asserts the examiner's interpretation is overly broad (Response at 46 & 47), but the examiner addressed this issue in Section 3.2.A and B above.

The patent owner also maintains that RFC 2230 fails to describe "any interaction between the DNS Server and the alleged 'DNS components' beyond the mere operation of running a DNS lookup." (Response at 47). The examiner does not agree. RFC 2230 teaches that the security extension to DNS (i.e., DNS-sec) (as described in RFC 2065, of record in this proceeding) stores signed public keys in the DNS. Section 1. RFC 2230 further teaches the "KX record is useful in providing an authenticable method of delegating authorization for one node to provide key exchange services on behalf of one or more, possibly different, nodes." *Id.* Thus, the DNS system delegates key exchange to a node. The delegatee (the key exchange node) still however acts on behalf of the delegator (DNS) rather than becoming an independent entity. Not surprisingly then, RFC 2230 subsequently teaches repeatedly that the initiator must query the

DNS with normal and/or reverse DNS lookups in order to determine (via KX records) which node R1 or R2 is authorized on behalf of the DNS system to act as a key exchanger. (Section 2.1.1, page 3; section 2.1.2, pages 4 & 5; and section 2.1.3, page 6). Thus, regardless of the definition of "delegate," RFC 2203 explicitly teaches that key exchange nodes (edge routers R1 and R2) are intertwined with the DNS system. See also the Fratto Declaration, ¶ 73-76.

The patent owner argues RFC 2230 fails to incorporate RFC 2065 (Response at 48), but the examiner disagrees for the reasons set forth in section 3.3B above. The patent owner's position is at odds with how the examiner believes one of ordinary skill in the art of Internet communications would interpret a prior art document citing to a RFC for protocol details.

The patent owner also alleges the routers R1 and R2 (key exchange nodes) act on behalf of nodes S and D not on behalf of the DNS system." RFC 2230 however states "the 'KX record is useful in providing an authenticable method of delegating authorization for one node to provide key exchange services on behalf of one or more, possibly different, nodes." (RFC 2230 at § 1). RFC 2230 teaches that the security extension to DNS (i.e., DNS-sec) (as described in RFC 2065, of record in this proceeding) stores keys in the DNS. (*Id.*) Thus, RFC 2230 teaches the KX record provides a method for delegating DNS key-exchange services to the routers R1 and R2 (key exchange nodes). As noted by the requester, RFC 2230 at § 2.1.1 also states "[i]n this example, R1 makes the policy decision to provide the IPSec service for traffic from R1 destined for R2. Once R1 has decided that the packet from S to D should be protected, it performs a secure DNS lookup for the records associated with domain D." Thus, router R1 is

not acting on behalf of S and D, but rather independently in order to determine how to route traffic between them including DNS lookup. See also the third party requester's remarks. (Comments at 41).

The patent owner also asserts that the establishment of the IPSec security association (VPN) does not indicate that the secure DNS system supports establishing a secure communication link. (Response at 48 & 49). This assertion however is premised claim interpretation arguments already addressed by the examiner. See section 3.1. Establishment of a VPN by routers R1 and R2, which are known to be part of (delegates) the DNS, is a discernible indication to the user that the DNS supports establishing a secure communication.

3.9.B Claims 18 and 42

The patent owner sets forth arguments (Response at 52 & 53) previously addressed above. The patent owner also asserts the Office improperly interprets the claim term "reserved," which is addressed in Section 3.3E above.

3.9.C. Claims 24 and 48

The patent owner sets forth arguments (Response at 53) previously addressed above. The patent owner also asserts the Office improperly asserts the claim are directed to nonfunctional descriptive material, which is addressed in Section 3.3.F above.

3.9.D. Claims 26 and 50

The patent owner asserts the "enable" limitation equates to a user action, such as clicking the mouse. (Response at 51).

The Larson patent under reexamination however 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... " (*Markman* at 27). Moroever, 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.

3.9.E. Remaining Arguments Regarding RFC 2230

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

3.10. Response to Patent Owner and Third Party Requester Comments Regarding RFC 2230 in view of RFC 920, RFC 2230 in view of RFC 2401, RFC 2230 in view of RFC 2401 and Reed, RFC 2230 in view of Beser

The patent owner sets forth arguments previously addressed above.

3.11. Response to Patent Owner and Third Party Requester Comments Regarding RFC 2538

3.11.A. Claim 1

The patent owner remarks that RFC 2538 fails to disclose an entity that queries and obtains a CERT RR nor a method for retrieving the CERT RR from the DNS. (Response at 58 & 59).

RFC 2538 states the certificates are retrieved from a DNS. (§6). Thus, an entity queries and obtains the certificate resource record (CERT RR). RFC 2538 also describes a method for retrieving the CERT RR, such as by storing by them "under a domain name related to their subject." (§3 & 3.1). Indeed, one of ordinary skill in the art of Internet communications would have recognized that DNS resource records (RR(s)) are returned to a query initiator. RFC 2538 also teaches that the retrieved CERT RR includes a DNS-sec (DNS security extension) key tag,

which provides an indication that the DNS system supports the establishment of a secure communication using DNS-sec. As discussed above in regard to the rejections based on Solana, DNS-sec returns both the IP address and a public key in response to a conventional DNS query. Thus, the return of a DNS-sec public key for the establishment of a secure communication and also the establishment of a secure communication provide indications that the DNS system supports secure communications (i.e., DNS-sec). The examiner also agrees with the requester that Cert RR clearly "asserts the authenticity and integrity of the data content, thereby providing security" for the initiator of the query so that a virtual private connection can be securely established between the initiator and the target (indication of support for establishing a secure communication). (Fratto Declaration at ¶ 80).

The remaining patent owner remarks are based on claim interpretation issues addressed by the examiner in Sections 3.1 and 3.2.

3.11.B.Claims 18 and 42

The patent owner sets forth arguments (Response at 62) previously addressed above. The patent owner also asserts the Office improperly interprets the claim term "reserved," which is addressed in Section 3.3.E above.

3.11.C.Claims 26 and 50

The patent owner asserts the "enable" limitation equates to a user action, such as clicking the mouse. (Response at 62 & 63). The examiner addressed this issue in Section 3.1 and 3.5.B above.

3.12. 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, pp. 65-67. The Declaration by Robert Dunham Short III, filed on April 18, 2012 with the earlier 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." ¶ 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 50), 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 Solana, Provino, Beser, RFC 2230, and RFC 2538, 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 at ¶ 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 at ¶ 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. 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:
/S. L. W./
Primary Examiner, Art Unit 3992

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