



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 |
| 23630 | 7590 | 09/26/2012 | | |
| McDermott Will & Emery 600 13th Street, NW Washington, DC 20005-3096 | | | EXAMINER FOSTER, ROLAND G | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 3992 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 09/26/2012 | 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.



DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

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

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NUMBER 95/001,789.

PATENT NUMBER 7921211.

TECHNOLOGY CENTER 3900.

ART UNIT 3992.

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

**ACTION CLOSING PROSECUTION
(37 CFR 1.949)**

Control No.

95/001,789

Examiner

ROLAND FOSTER

Patent Under Reexamination

7921211

Art Unit

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 18 April, 2012

Third Party(ies) on 06 August, 2012

Patent owner may once file a submission under 37 CFR 1.951(a) within 2 month(s) from the mailing date of this Office action. Where a submission is filed, third party requester may file responsive comments under 37 CFR 1.951(b) within 30-days (not extendable- 35 U.S.C. § 314(b)(2)) from the date of service of the initial submission on the requester. **Appeal cannot be taken from this action.** Appeal can only be taken from a Right of Appeal Notice under 37 CFR 1.953.

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.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

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

PART II. SUMMARY OF ACTION:

- 1a. ☒ Claims 1-60 are subject to reexamination.
- 1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled.
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). The certified copy has:
☐ been received. ☐ not been received. ☐ been filed in Application/Control No _____
10. ☐ Other _____

ACTION CLOSING PROSECUTION

1. Introduction

This Office action addresses claims 1-60 of United States Patent No. 7,921,211 B2 (the "Larson" patent), for reexamination was granted in the Order Granting *Inter Partes* Reexamination (hereafter the "Order"), mailed January 18, 2012.

A non-final Office action accompanying said Order was also mailed January 18, 2012 rejecting all original claims 1-60 of the Larson patent (the "non-final Office action").

The patent owner responded by filing arguments and associated evidence on April 18, 2012 (the "Response").

The third party requester responded by filing Comments to the Patent Owner's Response on August 6, 2012 (the "Comments"). In the Comments, the third party requester responded to the patent owner's arguments.

The examiner has carefully considered the arguments and evidence 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

Art Unit: 3992

maintained. Accordingly, this Office action is made an “**Action Closing Prosecution.**” See 37 CFR 1.949, MPEP 2671.02. See also the “conclusion” section to this Office action.

2. Prior Art Rejections

2.A. Issues Raised in the Request

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”).

Art Unit: 3992

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.B. 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.C. 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.D. 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 negated 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.

Art Unit: 3992

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.E. 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

Art Unit: 3992

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.

Art Unit: 3992

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.

Art Unit: 3992

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.F. 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.G. 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.H. 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

3.1. Prior Art Publication

The patent owner's arguments and associated evidence (Response, pp. 5-9) have been carefully considered, but the requester's evidence demonstrates that Solana, Reed, and the RFC(s) were printed publications available as prior art. Regarding Solana, Exhibit C to the Comments provides evidence that Solana was formally published in a treatise called "Lecture Notes in Computer Science" (LCNS) by Springer-Verlag in 1998. The declarant also attested to these facts. *See* the Declaration of Michael Allyn Fratto Under 37 C.F.R. 1.132, Fratto Declaration, filed with the Comments (the "Fratto Declaration"), paragraph 11. *See also* the Comments, p. 3. Regarding Reed, the same declarant presents evidence, such as the Association of Computing Machinery (ACM) website reporting the citation of Reed no later than December of 1996. Fratto Declaration, paragraphs 12-15. Regarding the RFC(s), these publications are among the most authoritative publications for Internet systems and protocols. The examiner agrees with the requester that "RFC documents are published and disseminated to the relevant public by the Internet Engineering Task Force (IETF) pursuant to a transparent and well-known process. Under these well-known procedures, RFCs are self-authenticating printed publications – each contain verifiable information documenting the date of its public distribution." Comments, pp. 3 & 4. Moreover:

Art Unit: 3992

Thus, the RFC documents cited in the Request and in the Office action would each have been published during the month and year that is listed in the heading of the RFC in accordance with IETF BCP 9. Each of these RFCs also would have been publicly distributed by the IETF and announced via their mailing list during the month and year listed in the heading of the RFC, and thus would have been publicly available without restriction as of the date noted on the document.

Fratto Declaration, paragraph 24. *See also* paragraphs 16-23.

The various RFC(s) identified in the Response, p. 8 are thus printed publications available as prior art during the month and year listed in the heading of the subject RFC.

3.2. Claim Interpretation

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

A system for providing a domain name service for establishing a secure communication link, the system comprising:

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

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

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

Regarding whether the DNS device is 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). The patent owner in their Response has not pointed to any language and arguments clearly disclaiming the embodiments discussed above that support this interpretation.

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

Art Unit: 3992

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”. Keromytis Declaration, paragraph 18. “DNS proxy 2610 then responds to the computer’s 2601 DNS request with an address received from the gatekeeper 2604.” *Id.* That is, rather than conventionally returning a public key to the initiator (e.g., computer 2601) so that the target and the initiator can establish a VPN, the special DNS server authenticates the request, then relies upon the services of a gatekeeper to receive an address (e.g., a “hopblock” address, col. 39, 67 – col. 40, l. 8) that the DNS server then provides to the initiator so that the initiator and target can establish a VPN. *See also* the Keromytis Declaration, paragraph 19.

The claims however do not recite a DNS “server” (as previously discussed) much less a DNS server that authenticates a user and relies upon the services of a gatekeeper, which is also consistent with the specification. Indeed in one embodiment, the patent owner states the DNS server (SDNS 3319) is queried “in the clear” (without using a VPN link) and without authenticating the user. Col. 51, ll. 37-50. The server then replies without the use of a gatekeeper 3314 “in the clear” so that the initiator and the target can establish a VPN. *Id.*

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

Art Unit: 3992

their Response has not pointed to any language and arguments clearly disclaiming the embodiments discussed above that support this interpretation.

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 Order, Ex. A. to the Comments, pp. 27 & 28.

3.3. The Solana Prior Art

3.3.A. Solana Teaches a “Domain Name Service System Configured to...Store Domain Names and Corresponding Network Addresses.”

The patent owner asserts Solana fails to teach a domain name server system configured to store a plurality of domain names and corresponding network addresses. First, it is argued, “Solana merely discloses that the DS stores “naming information and...certificates that securely bind domains to their public keys.” Response, p. 12. *See also* the Keromytis Declaration, paragraph 24. 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. Thus, the DNS-

Art Unit: 3992

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, paragraph 34.

Second, the patent owner argues the naming information is stored in Solana's DS "in the form of UNIs," which do not include both a domain name and a corresponding network address. Response, p. 12. *See also* the Keromytis Declaration, paragraph 25. The patent owner misinterprets the role of the UNI. 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

Art Unit: 3992

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 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, paragraphs 39-45.

Third, the patent owner asserts “one of ordinary skill in the art would not have understood Solana’s DS to be a domain name service system,” (*see also* the Keromytis

Art Unit: 3992

Declaration, paragraph 27) but as discussed above, Solana complies with DNS-sec (RFC 2065) and thus DNS (RFC 1034 and 1035).

3.3.B. Solana Teaches a “Domain Name Service System Configured to...Receive a Query for a Network Address.”

The patent owner argues Solana fails to disclose a DNS system configured to receive a query for a network address. Response, pp. 13-15. See also the Keromytis Declaration, paragraphs 30-36. The examiner does not agree. As previously discussed, the Solana DNS-Sec embodiment through incorporation of RFC(s) 1033, 1034, 1035 and 2065 teaches a DNS query specifying a domain name retrieves both a network address and a public key (if available). The patent owner's evidence does not address these teachings, especially in regard to RFC 2065, section 3.7. Regarding the patent owner's characterization of Figs. 2a and 2b (see the Keromytis Declaration, paragraphs 31-33), the examiner's agrees with the requester that these figures illustrate what happens after a query for network address is answered with a network address and public key for encryption/de-encryption. Fratto Declaration, paragraph 47.

3.3.C. Solana Teaches a “Domain Name Service System Configured...to... Indicate In Response To The Query Whether The Domain Name Service System Supports Establishing A Secure Communication Link.”

Independent Claims 1, 36 and 60 Are Not Patentable over Solana in View of RFC 2504

Dependent Claims 5, 23 and 47 are Not Patentable - Rejections Based on Solana

Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57 are Not Patentable - Rejections Based on Solana

The patent owner's arguments (Response, pp. 15-17, 41, 42, 49, 50) appear premised on the notion that Solana fails to disclose a DNS system storing domain names and corresponding network addresses and configured to receive a query for a network address, which is incorrect for the reasons previously explained in section 3.3.A above.

3.3.D. Dependent Claims 8 and 9 Are Not Patentable - Rejections Based on Solana

The patent owner argues that Solana only teaches that the organization “may use” virtual private networks, but “[i]t does not disclose or suggest that the alleged domain name service system (Solana’s DS) is connectable to a virtual private network.” Response, pp. 42 & 43. The examiner does not find this argument persuasive. Solana 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. Dependent Claims 18 and 42 Are Not Patentable - Rejections Based on Solana

The patent owner incorrectly asserts that the UNI is not reserved for secure communications links. Response, p. 53. 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

Art Unit: 3992

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).

3.3.F. Dependent Claims 24 and 48 Are Not Patentable – Rejections Based on Solana

The patent owner unpersuasively argues that Solana fails to teach “wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link.” Response, p. 56. 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

Art Unit: 3992

name to the establishment of a secure communications link. *See also* the Comments, pp. 10 & 11.

3.3.G. Dependent Claims 26 and 50 Are Not Patentable - Rejections Based on Solana

The patent owner incorrectly asserts that Solana fails to teach a domain name that enables establishment of a secure communication link. Pp. 61 & 62. 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 a 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 enables establishment of a secure communication link.

3.4. The Provino Prior Art

3.4.A. Provino Teaches a “Domain Name Service System Configured...to... Indicate In Response To The Query Whether The Domain Name Service System Supports Establishing A Secure Communication Link.”

The patent owner asserts the name server 17 fails to provide an “indication that the domain name service system support establishing a secure communication link.” Response, pp. 19-22. *See also* the Keromytis Declaration, paragraphs 44-46.

Art Unit: 3992

As an initial matter, the requester is correct in that the term “indication” has 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. Comment, p. 13, FN 6. *See also* the Markman Order, Ex. A., pp. 27 & 28.

The bulk of the patent owner’s arguments also incorrectly focus on name server 17 in Provino without addressing the role of the firewall 30 and VPN name server 32. The incorporated rejection indicated that more than just the acts of name server 17 were being relied upon in Provino. *See, e.g.*, the Request, p. 123. In focusing solely on the name server 17, the patent owner obscures the fact that 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). 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 3.2 above. The establishment of a secure connection between the query initiator (device 12(m)) and firewall 30 is an indication that the "domain service name service system 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

Art Unit: 3992

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.

The biggest structural difference between the Larson and Provino teachings discussed above is that, in Larson, the DNS proxy (server) 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.

The examiner also finds persuasive the requester's assertion that, even if name server 17 is incorrectly considered in isolation, it still provides an "indication" as claimed. Comments, pp. 13 & 14. As discussed above, name server 17 answers a 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. 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, 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

Art Unit: 3992

the "indication" as broadly claimed and consistent with the specification of the patent under reexamination. See also section 3.2 above for additional discussion regarding the recited term "indication."

The patent owner also asserts Provino fails to teach an indication that the "domain name service" supports establishing a communication link because the firewall 30 is not part of the domain name service. Pp. 22. The examiner disagrees. For the reasons discussed above (in this section), the firewall 30 forms a functional and structural part of a distributed DNS system consistent with the specification of the patent under reexamination. *See also* paragraphs 54 and 55 of the Fratto Declaration.

3.4.B. Provino Teaches a "Domain Name Service System Configured...to... Indicate In Response To The Query Whether The Domain Name Service System Supports Establishing A Secure Communication Link."

The patent owner contends *arguendo* that the "Internet address of the firewall 30 indicates that the name server 17 supports establishing as secure communication link as alleged (which it does not), the name server 17 does not provide the Internet address of the firewall 30 *in response to* this request to establish a secure tunnel the alleged query for a network address." Response, p. 23. Thus, it is argued, Provision fails to teach the indication (establishment of a secure communication link) "in response to the query" as required by the claims. *See also* the Keromytis Declaration, paragraphs 49 & 50.

The examiner does not agree. The incorporated rejections based on Provino do not rely on reading the "request to establish a secure tunnel" as the claimed query. The patent owner's position appears to be based on a misreading of Provino. For example, the patent owner argues "the only query or request *Provino* mentions in this passage [col. 9, ll. 46-60]...is a request sent from the device 12(m) to the firewall 30 to *establish a secure tunnel*." Response, p. 23. "In fact, device 12(m) sends the request to establish a secure tunnel to the firewall 30 *after* it has already received the Internet address of the firewall 30 from the name server 17. *Id.* However, the recited passage (col. 9, ll. 46-60) instead teaches name server 17 provides the Internet address of firewall 30 to device 12(m) (col. 9, ll. 46-57). Provino also teaches that name server 17 provides an Internet address when it receives a DNS request (query by domain name) from device 12(m) (col. 7, ll. 36-41). Thus, the Office reads the "query" on the DNS name query made by device 12(m) to name server 17, which returns the Internet address of secure firewall 30, which indicates a secure communications link can be established between device 12(m) and firewall 30. The indication thus occurs in response to the query.

The patent owner's remaining argument are premised on reading the query as the request sent by device 12(m) to firewall 30 to establish a secure connection, which as discussed above is incorrect.

3.4.C. Provino Teaches the Claimed Invention

The patent owner also argues Provino discloses a conventional DNS system (Response, pp. 24 and 25), but this is hardly the case. As discussed in section 3.4.A, Provino teaches an

Art Unit: 3992

unconventional DNS system comprising a DNS name server 17, firewall 30 and VPN server 32.

The DNS system provides an indication that the DNS "supports establishing a secure communication link" by establishing a secure connection between the query initiator and a firewall, providing the query initiator with the identification of a secure name server and the Internet address of a secure server.

3.4.D. Independent Claims 1, 36 and 60 Are Not Patentable - Provino in View of RFC 2230

Independent Claims 1, 36 and 60 Are Not Patentable - Provino in View of RFC 2504

The patent owner's arguments (Response, pp. 25-27) appear premised on the notion that Provino fails to disclose a DNS system configured to comprise an indication that the DNS system supports establishing a secure communication link, which is incorrect for the reasons previously explained in this section, subsection "A."

3.4.E. Dependent Claims 5, 23 and 47 Are Not Patentable - Rejections Based on Provino

The patent owner's arguments are unpersuasive in that they are premised on interpreting the request to establish a secure tunnel" as the claimed query the query, which is incorrect for the reasons discussed in this section, subsection "B."

3.4.F. Dependent Claims 8 and 9 Are Not Patentable - Rejections Based on Provino

Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57 Are Not Patentable - Rejections Based on Provino

The patent owner's arguments (Response, pp. 43, 44, 50 and 51) appear premised on the notion 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 this section, subsection "A."

3.4.G. Dependent Claims 24 and 48 Are Not Patentable - Rejections Based on Provino

The patent owner unpersuasively argues that Provino fails to teach "wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." Response, pp. 56 & 57. A "name" indicating that the DNS supports a secure communication link is nonfunctional descriptive material and thus cannot distinguish over the prior art. A "name" comprising an "indication" (as broadly recited) of support for a secure communications link is descriptive material directed to the mere arrangement of data. It is not a data structure (physical or logical relationships among data elements designed to support specific data manipulation functions) that defines a functional interrelationship to a secure communications function. MPEP 2106.01. In order to claim functional descriptive material, the claim should explicitly recite a data structure, such as a domain name comprising a secure top-level domain name (e.g., ".scom" Larson, col. 50, ll. 25-37) and explicitly recite a functional relationship that interrelates the secure top-level domain name to the establishment of a secure communications link. *See also* the Comments, p. 16.

Art Unit: 3992

3.4.H. Dependent Claims 26 and 50 Are Not Patentable - Rejections Based on Solana

The patent owner incorrectly asserts that Provino fails to teach a domain name that enables establishment of a secure communication link. Response, p. 62. As explained in section 3.4.A above, Provino teaches that DNS name server 17 responds to a query based on domain name by providing a network address for firewall 30. The firewall 30 then establishes a secure tunnel connection (VPN) with the query initiator device 12(m). The firewall 30 also provides device 12(m) with the identification of VPN nameserver 32 and secure server 31. A secure connection between device 12(m) and secure server 31 is then established. In such a case, the domain name enables establishment of a secure communication link.

3.5. The Beser Prior Art**3.5.A. Beser Teaches a "Domain Name Service System Configured...to... Indicate In Response To The Query Whether The Domain Name Service System Supports Establishing A Secure Communication Link."**

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." Response, p. 28. The patent owner alleges "*Beser* acknowledges that encryption exists, but teaches away from using it in the configuration disclosed by *Beser* because, according to *Beser*, encryption may provide insufficient protection, may be infeasible to implement, and/or may create service problems due to computer-power limitations." *Id.* See also the Keromytis Declaration, paragraph 64.

Art Unit: 3992

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, 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

Art Unit: 3992

address is more secure than encryption only. The claims however do not recite the degree of security. *See also* the Response, pp. 18-20 and the Fratto Declaration, paragraph 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, p. 26, Keromytis Declaration, paragraph 60. The examiner does not agree.

First, as discussed in section 1.2 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 Order, Ex. A. to the Comments, pp. 27 & 28. 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. 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

Art Unit: 3992

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 Comments, p. 21 and the Fratto Declaration, paragraph 66. Thus, Beser provides the "indication" as broadly claimed and consistent with the specification of the patent under reexamination.

The patent owner also contends Beser fails to disclose a query for a network address (Response, p. 29), but the third party requester is correct in noting Beser teaches the negotiation of private IP address is the purpose of the query (Comments, p. 21).

3.5.B. Dependent Claims 8 and 9 Are Not Patentable - Rejections Based on Beser

The patent owner asserts Beser and RFC 2401 fails to disclose that a "domain name service system is connectable to a virtual private network" as recited in claims 8 and 9. Response, pp. 44 & 45. The combination, it is argued, would "result in a virtual private network between the first and second network devices of Beser." *Id.* at 44. Beser however teaches queries to the trusted third party network device 30 "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." Col. 11, ll. 20-25. Encrypted and authenticated communications over a public network (e.g., Internet) is functionally equivalent to a virtual private network over the public network. Thus, Beser teaches

Art Unit: 3992

the DNS server (device 30) is connectable to a "virtual private network" as broadly claimed.

The device 30 may be a "back-end service...or distributed over several physical locations." Col. 11, ll. 33-36. RFC 2041 also teaches VPN edge routers pass through non-IPSec traffic to DNS servers. Section 4.4.1 and 5. Thus, the DNS server is connected to the VPN network behind the edge router (*i.e.*, traffic originating from the VPN network). See also the Comments, pp. 21 & 22 and the Fratto Declaration, paragraph 67.

3.5.C. Dependent Claims 18 and 42 are Not Patentable - Rejections Based on Beser

The patent owner asserts Beser fails to teach "at least one of the plurality of domain names is reserved for secure communication links," (Response, pp. 53 & 54), however the examiner agrees with the requester (Comments, p. 22) that when one of ordinary skill considers that certain domain names (unique identifiers) are associated with the first and second network devices for establishing a secure communication link, then those domains names are reserved for the secure communication link, although certainly the initiator is not required to then establish a secure communication link (*i.e.*, take advantage of the reservation).

3.5.D. Dependent Claims 24 and 48 Are Not Patentable - Rejections Based on Beser

The patent owner unpersuasively argues that Beser fails to teach "wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." Response, pp. 22 and 23. 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

Art Unit: 3992

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. 13-33) and explicitly recite a functional relationship that interrelates the secure top-level domain name to the establishment of a secure communications link. *See also* the Comments, pp. 23 & 24 and the Fratto Declaration, paragraph 69.

3.5.E. Dependent Claims 26 and 50 Are Not Patentable - Rejections Based on Beser

The patent owner incorrectly asserts that Beser fails to teach a domain name that enables establishment of a secure communication link. As explained in section 3.5.A above, Beser teaches that the DNS server (trusted network device 30) responds to a domain name query by negotiating and providing private addresses that result in the establishment of a communications link between the requester and target. The communications link is not only encrypted, but that has the source addresses hidden. In such a case, the domain name enables establishment of a secure communication link.

3.6 The RFC 2230 Prior Art

3.6.A. RFC 2230 Teaches a “Domain Name Service System Configured...to... Indicate In Response To The Query Whether The Domain Name Service System Supports Establishing A Secure Communication Link.”

The patent owner asserts RFC 2230 fails to teach that the KX resource record is an, "indication that the domain name service supports establishing a secure communication link" because delegated key exchanger nodes (edge routers R1 and R2) "are separate from the alleged domain name service system to which the DNS lookup was sent and from which the KX record was obtained. Response, p. 32. *See also* the Keromytis Declaration, paragraph 72.

The patent owner's remarks are not persuasive. 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

Art Unit: 3992

and R2) are intertwined with the DNS system. See also the Comments, pp. 24 & 25 and the Fratto Declaration, paragraphs 73-76.

The patent owner also asserts that the establishment of the IPSec security association does not indicate that the secure DNS system supports establishing a secure communication link. Response, p. 33. This assertion however is premised on the statement "As discussed above, however, a KX record does not comprise an indication that the alleged *domain name service system* supports establishing a secure communication link, as recited in claim 1." *Id.* The examiner however finds this premise unpersuasive. The key exchanger nodes R1 and R2 pointed to by the KX records in the DNS sever are part of the DNS system for the reasons discussed above in this section. Moreover, the term "indication" can be interpreted broadly consistent with the specification of the patent under reexamination, as discussed in sections 3.2, 3.4.A. and 3.5.A above.

The patent owner contents RFC 2230 fails to teach a query for a network address as required by the claims (Response, pp. 34 and 35), but as discussed above, RFC 2230 repeatedly teaches that the initiator "S" must query the DNS with normal DNS lookups in order to determine (via KX records) which node (e.g., "R2") acts as the key exchanger for destination "D". In order for node "S" to communicate with nodes "R2" and "D", then the DNS conventionally returns the Internet address based on a domain query. *See e.g.*, RFC(s) 1034 and 1035. Note that RFC(s) 1034 and 1035 are incorporated by RFC 2230. Specifically, RFC 2230 teaches a method for delegating key exchange authorization in DNS systems that support

Art Unit: 3992

security extensions as explained in to DNS (i.e., DNS-sec), where RFC 2230 identifies “RFC-1305, RFC-1034” as examples of the conventional DNS system and “RFC-2065” as an example of the security extensions to DNS (DNS-sec). Thus, RFC 2230 incorporates RFC(s) 1034, 1035 and 2065. Moreover, RFC 2065 incorporates RFC(s) 1034 and 1035. Abstract and section 1. Section 1. Also note that RFC 2230 explicitly teaches that “KX records MUST cause type A additional section processing for the host specified by EXCHANGER.” Section 3.1. Type “A” resource records (“RR”) contain the IP address corresponding to the queried domain name. *See, e.g., RFC 1034, sections 3.6. 3.7, 3.7.1.* Finally, a discussed in section 3.3.A above, the incorporated RFC 2065 teaches in DNS-sec that a conventional DNS query specifying a domain name returns both the IP address and a public key if space is available in the type “A” RR. *See also the Fratto Declaration, paragraph 75.*

The patent owner also argues RFC 2230 discloses a conventional DNS system (Response, pp. 35 & 36), but this is hardly the case. RFC 2230 teaches a method for delegating key exchange authorization in DNS systems that support security extensions as explained in to DNS (i.e., DNS-sec) (RFC 2065). RFC 2230 thus incorporates DNS-sec (RFC 2065). As discussed in section 3.3.A, DNS-sec (RFC 2065) teaches a DNS system that can queried using a domain name in order to retrieve the network address and the corresponding public key (if it exists) attached to the address thereby indicating support for the establishment of a secure communications link.

3.6.B. Dependent Claims 8 and 9 are Not Patentable - Rejections Based on RFC 2230

Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57 are Not Patentable -
Rejections Based on RFC 2230

The patent owner's arguments (Response, pp. 45, 46, 51 and 52) appear premised on the notion that, in RFC 2230, the key exchanger nodes (e.g., R1 and R2) are separate from the DNS system, which is incorrect for the reasons previously explained in section 3.6.A above.

3.6.C. Dependent Claims 18 and 42 are Not Patentable - Rejections Based on RFC 2230

The patent owner asserts RFC 2230 fails to teach “at least one of the plurality of domain names is reserved for secure communication links,” (Response, pp. 54 & 55), however the examiner agrees with the requester that when one of ordinary skill considers that certain domain names are stored within the DNS system are associated with KX records, then those domains names are 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).

3.6.D. Dependent Claims 24 and 48 Are Not Patentable - Rejections Based on RFC 2230

The patent owner unpersuasively argues that RFC 2230 fails to teach “wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link.” Response, pp. 59 & 60. 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

Art Unit: 3992

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* the Comments, p. 28 and the Fratto Declaration, paragraph 70.

3.6.E. Dependent Claims 26 and 50 Are Not Patentable - Rejections Based on RFC 2230

The patent owner incorrectly asserts that RFC 2230 fails to teach a domain name that enables establishment of a secure communication link. Response, pp. 63 & 64. As explained in section 3.6.A above, RFC 2230 teaches that the initiator must query the DNS system with a domain name query, where the response indicates via KX records which node R1 or R2 is authorized on behalf of the secure DNS system to act as a key exchanger for the establishment of a VPN connection. In such a case, the domain name enables establishment of a secure communication link. *See also* Comments, pp. 28 & 29 and the Fratto Declaration, paragraphs 75-78.

Art Unit: 3992

3.7. The RFC 2538 Prior Art**3.7.A. RFC 2538 Teaches a “Domain Name Service System Configured...to... Indicate In Response To The Query Whether The Domain Name Service System Supports Establishing A Secure Communication Link.”**

The patent owner asserts that the certificate in RFC 2538 "does not include any indication about the capabilities of the DNS server in which the certificate is stored" and the DNS server "does not support establishing a secure communication link -- it merely returns a certificate when one is requested." Response, p. 37 and the Keromytis Declaration, paragraph 86.

The patent owner's remarks are not persuasive. As discussed in section 3.2, the claims recite that a DNS **system**, which consistent with the specification means multiple devices and not necessarily a particular DNS server, supports establishing a secure communication. Thus, the patent owner's argument that the DNS server by itself must establish the VPN connection is directed to an unclaimed feature, which is unpersuasive. *See also* the Fratto Declaration, paragraph 79.

The examiner also agrees with the requester that the certificate response record ("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. Fratto Declaration, paragraph 80.

Moreover, even if the DNS sever providing the Cert RR is incorrectly considered in isolation, it still supports the establishment of a secure connection as broadly claimed and as

Art Unit: 3992

consistent with the specification of the patent under reexamination. Specifically, 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 to the query. *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. Thus, the actual establishment of the VPN completely bypasses the patent owners DNS server. Moreover as discussed, the DNS server in Larson provides an address as the indication of support for secure communications. Similarly in RFC 2538, the DNS server returns the Cert RR, which includes a certificate complying with X.509. An X.509 certificate contains the IP address of the public key's owner. *See* RFC 2459, section 4.2.1.7, of record in this proceeding. Thus, RFC 2538 similarly teaches providing an address as indication of support for secure communications (the public key is authenticated as belonging to the asserted owner). As the requester notes however, the release of a Cert RR by the DNS server by itself certainly indicates secure communications is supported for this particular transaction.

The patent owner contends RFC 2538 fails to teach indicating in response to a query for a network address as required by the claims (Response, p. 38), but as discussed above, the DNS server returns the Cert RR, which includes a certificate complying with X.509. An X.509 certificate contains the IP address of the public key's owner. *See* RFC 2459, section 4.2.1.7, of record in this proceeding. Obtaining the IP address is also one of the goal of the certificate query because the public key (received by the initiator from the asserted owner) must be authenticated

Art Unit: 3992

as actually belonging to the asserted owner (e.g., asserted IP address). See generally the incorporated X.509 protocol (RFC 2459) for verification of public key owners using certificates.

The patent owner also argues RFC 2538 discloses a conventional DNS system (Response, pp. 31-33), but this is hardly the case for the reasons discussed above. RFC(s) RFC(s) 1034 and 1035, of record in this proceeding, describe a conventional DNS system not RFC 2538. *See also* the Comments, pp. 31 and 32. Moreover, prior art may anticipate or render obvious a broadly claimed invention regardless of whether the prior art describes "conventional" technology.

3.7.B. Dependent Claims 8 and 9 are Not Patentable - Rejections Based on RFC 2538

Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57 are Not Patentable - Rejections Based on RFC 2538

The patent owner's arguments (Response, pp. 45, 46 & 52) appear premised on the notion that the DNS server in RFC 2538 does not support the establishment of a secure communication link, which is incorrect for the reasons previously explained in section 3.7.A above. See also the Comments, pp. 31 & 32 and the Fratto Declaration, paragraph 79.

3.7.C. Dependent Claims 18 and 42 are Not Patentable - Rejections Based on RFC 2538

The patent owner asserts RFC 2538 fails to teach "at least one of the plurality of domain names is reserved for secure communication links," (Response, p. 55), however the examiner

Art Unit: 3992

agrees with the requester that when one of ordinary skill considers that certain domain names are stored within the DNS system are associated with certificates, then those domains names are 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).

3.7.D. Dependent Claims 24 and 48 Are Not Patentable - Rejections Based on RFC 2538

The patent owner unpersuasively argues that RFC 2538 fails to teach “wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link.” Response, pp. 61 & 61. First, RFC 2538 does indeed teach that a domain names comprises an indication that the DNS system supports a secure communication link. See, e.g., section 3.1, example 1, “www.secure.john-doe.com.”

Nonetheless, 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

Art Unit: 3992

the secure top-level domain name to the establishment of a secure communications link. *See also* the Comments, pp. 32 & 33.

3.7.E. Dependent Claims 26 and 50 Are Not Patentable - Rejections Based on RFC 2538

The patent owner incorrectly asserts that RFC 2538 fails to teach a domain name that enables establishment of a secure communication link. As explained in section 3.7.A above, RFC 2538 teaches that the initiator must query the DNS system with a domain name query, where the response includes a Cert RR record containing a certificate that authenticates a public key as belonging to the asserted owner. As a result, a secure communications link based on public key encryption is established between the initiator and the target. In such a case, the domain name enables establishment of a secure communication link. *See also* Comments, pp. 33 & 34 and the Fratto Declaration, paragraphs 78 & 79.

3.8. The Prior Art Combination of Solana in view of RFC 2504

3.8.A. The Combination Based upon Solana in view of RFC 22504 Renders Claim's 1, 2, 5,6, 8, 9 and 14-60 Obvious.

The patent owner asserts that RFC 2504 fails to remedy the deficiencies of Solana and that, "Because RFC 2504 does not disclose a domain name service system, it does not disclose an indication that *the domain name service system* supports establishing a secure communication link...." Response, pp. 17 & 18. As explained in section 3.3.A however, the examiner does not find any deficiency in Solana to remedy. RFC 2504 need not teach a domain name service system that supports establishing a secure communication link because Solana does. The patent

Art Unit: 3992

owner's arguments are thus an attack on the references individually rather than on the combination.

3.9. The Prior Art Combination of Provino in view of RFC 2230

3.9.A. The Combination Based upon Provino in view of RFC 2230 Renders Claims 1, 2, 5, 6, 8, 9 and 14-60 Obvious.

The patent owner asserts that neither Provino or RFC 2230 teach the claimed indication in response to a query. Response, pp. 25 & 26. The examiner has previously discussed however how each of these references individually teach an indication in response to a query, thus the combination does as well. See sections 3.3.A and 3.6.A above.

3.10. The Prior Art Combination of Provino in view of RFC 2504

3.10.A. The Combination Based upon Provino in view of RFC 2230 Renders Claims 1, 2, 5, 6, 8, 9 and 14-60 Obvious.

The patent owner asserts that RFC 2504 fails to remedy the deficiencies of Provino and that, "Because RFC 2504 does not disclose a domain name service system, RFC 2504 cannot does not disclose an indication that the domain name service system supports establishing a secure communication link...." Response, pp. 26 & 27. As explained in section 3.4 however, the examiner does not find any deficiency in Provino to remedy. RFC 2504 need not teach a domain name service system that supports establishing a secure communication link because Provino does. The patent owner's arguments are thus an attack on the references individually rather than on the combination.

3.11. 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 "any of 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 with the Response, (the "Short Declaration") mentions some of the limitations in claims 1, 8, 9, 16 and 27, but then asserts the long-felt need was for a "system that could be easily and correctly used to enable secure communications." Paragraph 3. It is not clear how this highly generalized need specifically relate to the limitations of the mentioned claims (*nexus*), moreover nothing is stated about the remaining claims 2-7, 10-15, 17-26 and 28-60. For example, no claims recite the user "easily" and "correctly" enabling secure communications.

As noted by the requester (Comment, p. 37), 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

Art Unit: 3992

same, similar or different manner. The long-felt need must not have been satisfied by another before the invention by patent owner. MPEP 716.04.II.

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

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

4. Information Disclosure Statement

The Information Disclosure Statement (“IDS”) filed May 2, 2012 citing approximately 1,325 references, has been considered. The examiner however notes that MPEP 2656, under the heading “Prior Art Patents and Printed Publications Reviewed by Examiner in Reexamination” states, in part (emphasis added):

Art Unit: 3992

Where patents, publications, and other such items of information are submitted by a party (patent owner or requester) in compliance with the requirements of the rules, the **requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information.** The initials of the examiner placed adjacent to the citations on the form PTO/SB/08A and 08B or its equivalent, without an indication to the contrary in the record, do not signify that the information has been considered by the examiner any further than to the extent noted above.

Additionally, MPEP 609.05(b) states (emphasis added):

The information contained in information disclosure statements which comply with both the content requirements of 37 CFR 1.98 and the requirements, based on the time of filing the statement, of 37 CFR 1.97 will be considered by the examiner. Consideration by the examiner of the information submitted in an IDS means that **the examiner will consider the documents in the same manner as other documents in Office search files are considered by the examiner while conducting a search of the prior art in a proper field of search.** The initials of the examiner placed adjacent to the citations on the ** PTO/SB/08A and 08B or its equivalent mean that the information has been considered by the examiner to the extent noted above.

With this, the examiner notes that the approximately 1,325 prior art references listed in said IDS have been considered by the examiner to at least the “degree to which the party filing the information citation has explained the content and relevance of the information,” and in “the same manner as other documents in Office search files are considered by the examiner while conducting a search of the prior art in a proper field of search” (see attached PTO/SB/08A’s).

5. Conclusion

This is an ACTION CLOSING PROSECUTION (ACP); see MPEP § 2671.02.

Art Unit: 3992

- (1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.
- (2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).
- (3) Appeal **cannot** be taken from this action, since it is not a final Office action.

Any paper filed with the USPTO, i.e., any submission made, by either the Patent Owner or the Third Party Requester must be served on every other party in the reexamination proceeding, including any other third party requester that is part of the proceeding due to merger of the reexamination proceedings. As proof of service, the party submitting the paper to the Office must attach a Certificate of Service to the paper which sets forth the name and address of the party served and the method of service. Papers filed without the required Certificate of Service may be denied consideration. 37 CFR 1.903; MPEP 2666.06.

Any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR 1.52(a) and (b), and must contain any fees required by 37 CFR 1.20(c). Amendments in an *inter partes* reexamination proceeding are made in the same manner that amendments in an *ex parte* reexamination are made. MPEP 2666.01. See MPEP 2250 for guidance as to the manner of making amendments in a reexamination proceeding.

Extensions of time under 37 CFR 1.136(a) will not be permitted in *inter partes* reexamination proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to the patent owner in a reexamination proceeding. Additionally, 35 U.S.C. 314(c)

Art Unit: 3992

requires that *inter partes* reexamination proceedings “will be conducted with special dispatch” (37 CFR 1.937). Patent owner extensions of time in *inter partes* reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner’s response is set by statute. 35 U.S.C. 314(b)(3).

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 patent undergoing reexamination or any related patent throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly inform the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

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

By Mail to: Mail Stop *Inter Partes* Reexam
 Attn: Central Reexamination Unit
 Commissioner of Patents
 United States Patent & Trademark Office
 P.O. Box 1450
 Alexandria, VA 22313-1450

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

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

By EFS-Web:

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
Central Reexamination Unit, Primary Examiner
Electrical Art Unit 3992
(571) 272-7538

Conferee: /BJP/

Conferee: /DJR/