

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re <i>Inter Partes</i> Reexamination of)	
U.S. Patent No. 7,418,504)	Control No.: 95/001,788
Larson et al.)	Group Art Unit: 3992
Issued: August 26, 2008)	Examiner: Roland Foster
For: AGILE NETWORK PROTOCOL FOR)	Confirmation No.: 5823
SECURE COMMUNICATIONS)	
USING SECURE DOMAIN NAMES)	

COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. § 1.947

Mail Stop **Inter Partes Reexam**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Third Party Requester Apple Inc. (“Apple”) submits these comments responsive to Patent Owner’s Response dated December 26, 2012 (“Second Response”) and the Action Closing Prosecution (“ACP”) dated September 26, 2012. For the convenience of the Office, a table of comments is provided at pages (i) to (v). Comments begin on page 1.

TABLE OF CONTENTS

I. BACKGROUND	1
II. RESPONSE TO PATENT OWNER CONTENTIONS REGARDING CLAIM CONSTRUCTIONS	1
A. Patent Owner Does Not Understand the Purpose or Effects of the Office’s “Broadest Reasonable Construction” Policy.....	2
B. The Office’s Construction of “Domain Name Service System” Is Correct.....	3
C. The Construction of “Indication” by the Office Was Correct.....	4
III. THE REJECTIONS OF THE CLAIMS WERE PROPER.....	6
A. Response to Patent Owner’s Arguments Regarding Rejection of Claims 1, 2, 5, 6, 8-9, and 14-60 as Anticipated by <i>Solana</i> (Issues 1-8).....	6
1. Independent Claims 1, 36, and 60.....	6
a. <i>Solana</i> Discloses “a Domain Name Service System Configured to . . . Comprise an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link.”	6
b. <i>Solana</i> Describes DNS Systems that Store a Plurality of Domain Names and Corresponding Network Addresses and That Receive Requests for a Network Address.....	9
2. Dependent Claims 5, 23, and 47 (Issue Nos. 1, 2, 5, 6).....	11
3. Dependent Claims 8 and 9 (Ground Nos. 1, 5).....	13
4. Dependent Claims 16, 17, 27, 33, 40, 41, 51, and 57 (Ground Nos. 1, 5).....	14
5. Dependent Claims 18 and 42 (Ground Nos. 1, 5).....	14
6. Dependent Claims 24 and 48 (Ground Nos. 1, 2, 5, 6).....	14
7. Dependent Claims 26 and 50 (Ground Nos. 1, 5).....	16
8. Dependent Claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59 (Ground Nos. 1-8).....	16
B. Rejection of Claims 2-5, 24, 25, 37, 48 and 49 Based on <i>Solana</i> in view of RFC 920 (Issue No. 2).....	16
C. Rejection of Claims 10-13 Based on <i>Solana</i> in view of <i>Reed</i>, or <i>Solana</i> in view of RFC 2504 and <i>Reed</i> (Issue No. 7).....	16
D. Rejection of Claims 7, 32, and 56 Based on <i>Solana</i> in view of <i>Beser</i> (Issue No. 4) 18	
E. Rejection of Claims 1, 2, 5, 6, 8, 9, and 14-60 Based on <i>Solana</i> in view of RFC 2504 (Issue No. 5)	18
F. Rejection of Claims 2-5, 24, 25, 37, 48, and 49 Based on <i>Solana</i> in view of RFC 2504 and RFC 920 (Issue No. 6)	18

G. Rejection of Claims 7, 32, and 56 Based on *Solana* in view of RFC 2504 and *Beser* (Issue No. 4).....18

IV. REJECTION OF CLAIMS 1-2, 5-6, 8-9, AND 14-60 UNDER 35 U.S.C. § 102(B) BASED ON *PROVINO* (ISSUE NO. 9)..... 18

A. Response Concerning Independent Claims 1, 36, and 6018

 1. *Provino*'s "Firewall 30" is Plainly a Functional Component of the *Provino* DNS Systems 19

 2. *Provino* Teaches DNS Systems that Comprise an "Indication" Specified in Claims 1, 36 and 60..... 22

B. Response Concerning Dependent Claims 5, 23, and 47.....25

C. Response Concerning Dependent Claims 8 and 9 (Ground Nos. 1, 5).....26

D. Response Concerning Dependent Claims 24 and 48 (Ground Nos. 1, 2, 5, 6).....27

E. Response Concerning Dependent Claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-5928

F. Rejection of Claims 2-5, 24, 25, 37, 48 and 49 Based on *Provino* in view of RFC 920 (Issue No. 10).....28

G. Rejection of Claims 10-13 Based on *Provino* in view of *Reed* (Issue No. 11)28

H. Rejection of Claims 7, 29-32, and 53-56 Based on *Provino* in view of *Beser* (Issue No. 12)29

I. Rejection of Claims 1, 2, 5, 6, 8, 9 and 14-60 Based on *Provino* in view of RFC 2230 (Issue No. 13)29

J. Rejection of Claims 2-5, 24, 25, 37, 48 and 49 Based on *Provino* in view of RFC 2230, in further view of RFC 920 (Issue No. 14).....29

K. The Rejection of Claims 10-13 Based on *Provino* in view of RFC 2230, and in further view of *Reed* (Issue No. 15) Was Proper29

L. The Rejection of Claims 7, 29-32, and 53-56 Based on *Provino* in view of RFC 2230, and in further view of *Beser* (Issue No. 16) Was Proper30

M. Rejection of Claims 1, 2, 5, 6, 8, 9, and 14-60 Based on *Provino* in view of RFC 2504 (Issue No. 17).....30

N. Rejection of Claims 2-5, 24, 25, 37, 48, and 49 Based on *Provino* in view of RFC 2504 and RFC 920 (Issue No. 18)30

O. The Rejection of Claims 10-13 Based on *Provino* in view of RFC 2504, and in further view of *Reed* (Issue No. 19) Was Proper31

V. REJECTION OF CLAIMS 1-2, 5-6, 8-9, AND 14-60 UNDER 35 U.S.C. § 102(B) AND §103 BASED ON *BESER* (GROUND NO. 21)..... 31

A. Independent Claims 1, 36, and 6031

1. *Beser* Teaches Its DNS Systems Can and Do Use Encryption, and Do Not “Teach Away” from the Claimed DNS Systems..... 32

2. *Beser* Teaches a DNS System that Comprises an “Indication” Specified in Claims 1, 36, and 60..... 35

B. Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57 (Issue No. 21)36

C. Dependent Claims 18 and 42 (Issue No. 21)36

D. Dependent Claims 24 and 48(Issue Nos. 21 and 22)37

E. Dependent Claims 26 and 50 (Issue No. 21)37

F. Dependent Claims 2, 5-7, 14, 15, 19-23, 25, 28-32, 34, 35, 37-39, 43-47, 49, 52-56, 58, and 59 (Issue No. 21).....38

G. Dependent Claims 2-5, 24, 25, 37, 48, and 49 (Issue No. 22).....38

H. Dependent Claims 8 and 9 (Issue No. 23)38

I. Dependent Claims 10-13 (Issue No. 24)38

VI. RESPONSE TO PATENT OWNER’S ARGUMENTS REGARDING REJECTION OF CLAIMS 1-2, 5-6, 8-9, AND 14-60 BASED ON RFC 2230 (ISSUE NO. 25)..... 39

A. Independent Claims 1, 36, and 6039

1. RFC 2230’s Routers “R1” and “R2” Are Plainly A Functional Component of the RFC 2230 DNS Systems..... 39

2. RFC 2230 Discloses “a Domain Name Service System Configured to . . . Comprise an Indication...” 42

B. Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57.....42

C. Dependent Claims 18 and 42.....42

D. Dependent Claims 24 and 48.....43

E. Dependent Claims 26 and 50.....43

F. Dependent Claims 2, 6, 14, 15, 19-23, 25, 27, 28-32, 34, 35, 37-39, 43-47, 49, 50, 52-56, 58, and 59.....44

G. Rejection of Dependent Claims 2-5, 24, 25, 37, 48, and 49 Based on RFC 2230 in View of RFC 920 (Issue No. 26).....45

1. Dependent Claim 5 45

2. Dependent Claims 24 and 48 45

H. Rejection of Dependent Claims 8 and 9 Based on RFC 2230 in View of RFC 2401 (Issue No. 27)46

I. Rejection of Claims 10-13 based on RFC 2230 in View of RFC 2401 and in Further View of *Reed* (Issue No. 28)46

J. Rejection of Claims 29-32 and 53-56 Based on RFC 2230 in view of *Beser* (Issue No. 29)46

VII. REJECTION OF CLAIMS 1, 2, 6, 14-22, 24-46, 48-52, AND 57-60 UNDER 35 U.S.C. § 102(B) BASED ON RFC 2538 (ISSUE NO. 30) 47

A. Independent Claims 1, 36, and 6047

B. Dependent Claims 16, 17, 27, 33, 40, 41, 51, and 57.....47

C. Dependent Claims 18 and 42.....48

D. Dependent Claims 26 and 50.....48

E. Rejection of Claims 3, 4, 24, 25, 48, and 49 Based on RFC 2538 in View of RFC 920 (Issue No. 31).....49

F. Rejection of Claims 8 and 9 Based on RFC 2538 in View of RFC 2401 (Issue No. 32)49

G. Rejection of Claims 10-13 Based on RFC 2538 in view of RFC 2401 in Further View of Reed (Issue No. 33).....49

H. Rejection of Claims 29-32 and 53-56 Based on RFC 2538 in View of *Beser* (Issue 34)49

I. Rejection of Claims 5, 23, and 47 based on RFC 2538 in View of RFC 2065 (Issue 35)49

VIII. THERE ARE NO SECONDARY CONSIDERATIONS LINKED TO THE CLAIMS 50

I. Background

On March 29, 2012, Patent Owner filed an overlength response (“First Response”) to the December 29, 2011 Office action (“First Action”). On June 25, 2012, Requester filed a 50-page response with comments (“Comments”) on Patent Owner’s response. On September 26, 2012, the Office issued an ACP that found claims 1-60 of U.S. Patent No. 7,418,504 (“the ’504 patent”) unpatentable. On December 26, 2012, the Patent Owner filed its Second Response and a petition under 37 C.F.R. § 1.183 seeking to waive the page limit rule for that response. Although the Office has not acted on the page-limit waiver as of the date of this submission, Requester provides these comments now to expedite conclusion of this proceeding. Requester believes no fee is due for this response, but authorizes the Director to debit any fee determined to be necessary from Deposit Account No. 18-1260.

Requester notes that Patent Owner submitted a Supplemental Declaration of Angelos D. Keromytis, Ph.D. with its Second Response, but did not establish good and sufficient reasons why this affidavit is necessary or could not have been presented earlier. On January 10, 2013, Requester petitioned the Director to not admit this Supplemental Declaration as it is barred by 37 CFR § 1.116(e) (affidavit may not be admitted after an ACP without “good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented.”) As explained in that petition, nowhere in its Second Response does Patent Owner even attempt to comply with Rule 1.116(e). Indeed it cannot – the Second Response simply rehashes arguments Patent Owner and its expert presented earlier, advances unsupportable *legal* theories about its claims, or attempts, for the first time, to address issues that were ripe for response after the First Action. The Examiner consequently should not admit or consider the new evidence or arguments presented in the Supplemental Declaration.

II. Response to Patent Owner Contentions Regarding Claim Constructions

On pages 1-8 of its Second Response, Patent Owner presents general challenges to the rejections in the ACP, contending the Office’s constructions of the claims are “defective” based on “incorrect positions on claim constructions,” and that constructions applied by the Office are “effectively new claim-constructions positions” for which the “Patent Owner has not had a chance to rebut.” Second Response at 1-2. Patent Owner is incorrect on each point. The “effectively new claim-constructions positions” are not new at all – they are the same ones proposed in the Request and used by the Office in the First Action. Moreover, contrary to Patent

Owner's contentions, these constructions are technically accurate and reflect the broadest reasonable construction of the claims, as explained below.

A. Patent Owner Does Not Understand the Purpose or Effects of the Office's "Broadest Reasonable Construction" Policy

Patent Owner repeatedly acknowledges that the claims must be given their "broadest reasonable construction" in this proceeding. Patent Owner's comments, however, demonstrate it does not understand the implications in this case of this well-established Office policy. Specifically, Patent Owner asserts the Examiner has improperly interpreted the claims, and demands that the claims be read in a manner that would exclude from their actual scope – as defined by the words used in the claims – subject matter which (i) Patent Owner has "clearly and unequivocally disclaims" or which the "specification repeatedly and explicitly disparages," and (ii) which differs from specific embodiments described in the specification. Second Response at 5. Patent Owner believes it is appropriate to read limitations into its claims based on the "unmistakable disavowal[s] of claim scope" that it made. *Id.* at 8.

Patent Owner's criticisms reflect its fundamentally flawed understanding of the Office's policy of giving the claims their broadest reasonable construction. In proceedings before the Office, a patent owner must amend the claims to effectively exclude subject matter actually encompassed by the claim language. See MPEP § 2111 (explaining that under the broadest reasonable construction practice used in PTO proceedings, "... applicant has the opportunity to amend the claims during prosecution, [and that] giving a claim its broadest reasonable interpretation will reduce the possibility that the claim, once issued, will be interpreted more broadly than is justified.") (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)). This practice is fundamentally different than claim construction before a court, where a patent owner cannot amend its claims. In the latter process, courts may consider clear disclaimers and other statements made by the Patent Owner during prosecution of the patent to construe the claims. Those judicial claim construction mechanisms, however, have no role in proceedings before the Office, because in this proceeding, the words in the claims can simply be changed to match the meaning the Patent Owner contends they should have. See M.P.E.P. § 2111 (construing *In re Morris*, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997) as providing that "PTO is not required, in the course of prosecution, to interpret claims in applications in the same manner as a court would interpret claims in an infringement suit.")

Patent Owner's arguments in this case vividly demonstrate why this rule is followed – all of Patent Owner's arguments seek to impermissibly import unclaimed limitations, requirements, meanings or “disclaimers” into the claims in order to narrow their scope and avoid the prior art, now that the claims have been found – based on their actual language – to encompass what is disclosed in or rendered obvious from the prior art. *See* M.P.E.P. § 2111.01(II); *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969) (“reading a claim in light of the specification, to thereby interpret limitations explicitly recited in the claim, is a quite different thing from ‘reading limitations of the specification into a claim,’ to thereby narrow the scope of the claim by implicitly adding disclosed limitations which have no express basis in the claim.”); *Superguide Corp. v. DirectTV Enterprises, Inc.*, 358 F.3d 870, 875, 69 USPQ2d 1865, 1868 (Fed. Cir. 2004) (“Though understanding the claim language may be aided by explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim. For example, a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment.”).

Indeed, by making these assertions, Patent Owner necessarily admits the claims actually encompass what the Office says they do. However, instead of seeking to amend the claims to correspond to the meaning(s) Patent Owner desires them now to have (and demonstrating there is written description support for these redefined methods and systems in its disclosure), Patent Owner asks the Office to simply ignore its well-established practices and do precisely what the MPEP and relevant rules state it should not – allow Patent Owner to import into the claims unclaimed limitations by reading the words as having special or narrow meanings, or by excluding from their actual scope subject matter Patent Owner putatively has “disparaged” or “disclaimed.” Allowing the Patent Owner to recast its claims without actually amending them would violate the Office's well-established practice of requiring a patentee to expressly incorporate limitations in the claim language to effectively limit their scope in these proceedings, and would prevent the Office and Requester from evaluating the newly claimed subject matter for compliance with 35 U.S.C. § 112. Consequently, Patent Owner's requests that the Office depart from its well-established practices must be uniformly rejected.

B. The Office's Construction of “Domain Name Service System” Is Correct

In the ACP, the Office correctly found that a Domain Name Service (or DNS) “System” is “reasonably interpreted as comprising a single device or multiple devices.” ACP at 15. In

support of this interpretation, the Office noted the '504 patent itself describes the DNS system as comprising multiple components, including “gatekeeper 2603, DNS proxy 2610 and DNS server 2609.” ACP at 15 (citing '504 patent at col.40, ll.35-48). The Office also agreed with Requester that the “DNS system according to the claim can be distributed across multiple computer systems.” ACP at 15 (citing Fratto Declaration, June 25, 2012, paragraph 30). In response, Patent Owner contends the Office improperly read this term to have “no bounds whatsoever.” Second Response at 3 (asserting Office “stretches th[e] understanding to contend that virtually any device—regardless of whether it has any DNS functionality—may be a ‘DNS device’ as long as it is in the same network as at least one device that actually has DNS functionality.”).

Patent Owner grossly misrepresents the Office’s statements, which were made in response to Patent Owner’s attempt in the First Response to improperly narrow the term “DNS system” to mean a “special and separate DNS device.” ACP at 16. The Office properly rejected that theory because nothing in the claim language or the '504 disclosure supports Patent Owner’s contentions. First, the claims recite simply “Domain Name Service System,” not a “special and separate DNS device.” The claims also contain no language specifying which devices may or may not be included in a “DNS system” and do not expressly or implicitly define specific “DNS functionalities” that each device must possess (e.g., to thus possess some undefined “DNS functionality.”) In fact, “DNS device” and “DNS functionality” appear nowhere in the claims.¹ Second, 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 Patent Owner (e.g., that a DNS system must consist of a particular set of components, all of which have “significant DNS functionality”). *See* Second Response at 4. Finally, Patent Owner’s argument is inconsistent with statements it made to the Court in concurrent litigation in Texas, where it asserted a “domain name service system” was simply “a computer system that includes a domain name service (DNS).” Markman Order, Ex. A to the Comments, at 19 (emphasis added). Patent Owner’s improper attempt to import unclaimed limitations into the claims via the term “DNS system” should be flatly rejected.

C. The Construction of “Indication” by the Office Was Correct

¹ Patent Owner also insists that the asserted references “contradict the Office’s overbroad construction of a ‘DNS device.’” Second Response at 4. But the Office did not construe “DNS device” which is a term that appears nowhere in the claims.

Patent Owner asserts the Office improperly construed the claim term “indication.” In the First Action, the Office found this term had a broad meaning, and encompassed a variety of types of events. First Action (Order) at 7, 10, 11. In the ACP, the Office elaborated on its findings, stating that, as the term is used in the claims, “indication” “*may be construed broadly to mean a visible message or signal to a user.*” ACP at 18 (emphasis added). The Office also pointed to examples in the specification of the ’504 patent that describe various methods of providing an “indication.” *See, e.g.*, ACP at 18 (citing col.41, ll.41-49) (observing a “request would result in *an indication of secure communication (establishment of a VPN).*”) (emphasis added). The Office thus confirmed that “indication” in its broadest reasonable construction encompasses a variety of types of indications, and that neither the language in the claims nor the specification limited the meaning of this term to one or a handful of particular types of indications. Consequently, the Office correctly found the term “indication” encompassed (but was not limited to) “a visible message or signal to user” and that such a message or signal could include “establishment of a VPN.” ACP at 18. The Office’s conclusions were consistent with explanations provided in the Request, which the Office relied upon and incorporated into the First Action. Request at 38-45. And, critically, in the ACP, the Office did not change any aspect of the rejections imposed in the First Action based on its comments about this claim term.

Despite this, Patent Owner complains that the Office has adopted a new construction for “indication” that is “inconsistent” with the specification. Specifically, Patent Owner asserts that an indication cannot reasonably be construed to be something “such as merely returning an IP address, a public key, or a certificate demonstrating authenticity of the source of the public key.” *Id.* at 5-6. Yet, here, Patent Owner is simply being duplicitous. Indeed, during the litigation, Patent Owner first contended that no construction was necessary for “indication” and, significantly, that the term should not be limited to “visible messages or signals to a user.” *Id.* Patent Owner also contended that an “indication” could be conveyed by provision of a certificate, stating that “in preparing devices for the FaceTime call, Apple’s Server(s) ensure that the participant devices have local iPhone security certificates...” VimetX Amended Infringement Contentions ’211 patent at 8 (emphasis added). Indeed, Patent Owner took the position that the term should not be limited or restricted by the patent specification, relying on Judge Davis’s general admonition that “[t]he specification’s disclosure or omission of examples does not create limitation on claims.” *See* Reply Markman Br. at 9. Against this backdrop, Patent

Owner cannot now argue (absent a claim amendment) that the broadest reasonable interpretation for “indication” excludes use of certificates, encryption keys, or similar security parameters that are returned to the requester, or that only an indication “visible to a user” can satisfy the broadest reasonable construction of the claims.

Patent Owner also responds with a number of irrelevant and unfounded criticisms. For example, Patent Owner suggests it has been prejudiced because the Office did not use only one of the possible meanings of an “indication” in every rejection that was imposed. This, Patent Owner complains, requires it to “guess as to the true basis of the rejection.” Patent Owner’s complaint is baseless. The Office employed its constructions in a manner dictated by the prior art being applied to the claims in each instance, and clearly explained how the prior art in each instance met the “indication” limitation in the claims. The rejections thus were clear and precise, and only through studied ignorance can Patent Owner contend otherwise.

III. The Rejections Of the Claims Were Proper

A. Response to Patent Owner’s Arguments Regarding Rejection of Claims 1, 2, 5, 6, 8-9, and 14-60 as Anticipated by *Solana* (Issues 1-8)

1. Independent Claims 1, 36, and 60

Solana describes domain name service systems (“DNS systems”) that establish secure communication links between an initiator (the source domain) and a responder (the destination domain). *See* Request at 39-46; ACP at 7. *Solana* also explains that its DNS systems are connected to a communication network, store a plurality of domain names and corresponding network addresses, receive queries for a network address and comprises an indication that it (i.e., the “domain name service system”) supports establishing secure communication links. *Solana* at 43-44. Consequently, the Office found that *Solana* describes “DNS systems” that anticipate independent claims 1, 36 and 60. In its Second Response, Patent Owner asserts the *Solana* DNS systems do not: (1) “comprise an indication that the domain name service system supports establishing a secure communication link or (2) “store domain names and corresponding network addresses” and “receive a query for network address.” Each assertion is incorrect.

a. ***Solana* Discloses “a Domain Name Service System Configured to . . . Comprise an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link.”**

In the ACP, the Office correctly found that *Solana* discloses “a Domain Name Service System configured to . . . comprise an indication that the domain name service system supports

establishing a secure communication link.” ACP at 22. This was consistent with the Office’s finding in the First Action that *Solana* satisfied the claimed “indication” in part through “the public keys and signatures (encryption keys) provide[d] by the DNSsec direction service.” First Action (Order) at 7. In the ACP, the Office also pointed out that Patent Owner had not specifically contested this finding about the “indication” in the first Office Action, but had simply stood by its incorrect position that the systems described in *Solana* are not “DNS systems.” *See, e.g.*, ACP at 22 (“[P]atent Owner’s arguments . . . appear premised on the notion that *Solana* fails to disclose a DNS system storing domain names and corresponding network addresse[s] and configured to receive a query for a network address, which is incorrect for the reasons previously explained.”). *See also* First Response at 16-18 (showing Patent Owner did challenged only whether such “indication[s]” were provided by a “DNS system.”).

Patent Owner now, in an untimely fashion, contends that *Solana* does not disclose an “indication” within the meaning of the claims. Patent Owner is incorrect – the *Solana* systems and processes show “indications” within the meaning of the claims for the reasons identified in the First Action, the ACP and in the Request. Request at 44-45; First Action at 5; ACP at 22. Patent Owner’s delay in advancing this new theory is explained by its strategy of portraying the claims in one manner before the Office, but in a fundamentally different manner before the courts. Specifically, Patent Owner, when it submitted its First Response, was contending to the Court in Texas that the use of security certificates in verifying identity and otherwise securing the communication link constitutes an “indication” within the meaning of the claims. *See, e.g.*, VirnetX Amended Infringement Contentions ’504 patent at 7 (“[I]n preparing devices for the FaceTime call, Apple’s Server(s) ensure that the participant devices have local iPhone security certificates . . .”) (emphasis added); *see also* January 5, 2012 Markman Transcript at 102 (“[The indication] could be as simple as the domain name service system responding to the software modules that initiated the query to say we are good to go and have our secure communication now.”). Now, with the District Court trial over, and facing the rejection of these claims, Patent Owner reverses course and attempts to introduce a new restrictive meaning for “indication” under the guise of an improper or misapplied claim construction by the Office. As described above, the Office’s interpretation of “indication” was correct, and there is no basis for withdrawing the rejection of the claims of the ’504 patent.

Patent Owner also contends that (1) the Office does not “demonstrate how *Solana* discloses an ‘indication’” (and in particular how *Solana*’s use of “certificates and encryption keys” constitute an “indication”) and (2) “*Solana* . . . does not disclose the recited ‘indication’ under a broadest reasonable interpretation.” Again, both points are incorrect.

The first assertion is simply false. The Request, which the Office incorporated into the first Office Action, presented a detailed analysis of how the use of “certificates and encryption keys” in the methods and systems described in the *Solana* reference met the “indication” claim requirement. Request at 38, 44-45. Patent Owner did not challenge this description of *Solana* in its First Response or that *Solana* met the claimed “indication” requirement. It cannot now contend this uncontested previous finding of the Office was somehow defective.

Patent Owner’s second assertion is also incorrect. Here, Patent Owner’s main theory appears to be that because it “disparaged” the “certificate/key architecture” as being known in the art, and because the *Solana* systems use certificates and keys, the *Solana* systems cannot disclose the claimed “indication.” Second Response at 9-10. As Patent Owner must be aware, nearly all inventions are combinations of known components. In *Solana*, particular uses of the certificates and of a public/private key architecture are described – *Solana* is not cited to prove simply that certificates and public key architecture was known. Instead, because *Solana* uses certificates and a key architecture in a manner that is the same as that specified in the claims, these uses of certificates and keys constitute “indications” within the meaning of the claims. Moreover, Patent Owner does not explain *how* the uses of certificates and keys in the *Solana* processes and systems relate to its “disparagement” of uses of these technologies in other, unrelated processes and systems. Finally, as noted above, there is no legal theory that permits a patent owner in a reexamination proceeding to secure patent claims that, by their actual claim language, encompass the prior art by simply pointing to “disparaging” remarks about the technology that the claims literally encompass. Instead, to effectively distinguish the claims from the prior art in these proceedings, the language in the claims has to be changed to expressly exclude that prior art subject matter from their scope. As Patent Owner has not sought to amend the claims to exclude the subject matter it putatively “disparaged,” its theory is irrelevant and must be ignored. Thus, because *Solana* describes DNS systems that provide an “indication” as required by the claims, the Examiner’s finding of anticipation of claims 1, 36 and 60 was proper.

b. *Solana* Describes DNS Systems that Store a Plurality of Domain Names and Corresponding Network Addresses and That Receive Requests for a Network Address

The Office correctly found that *Solana* discloses both “a domain name service system configured to . . . store a plurality of domain names and corresponding network addresses” and that the system receives requests for a network address. First Action at 5-7; ACP at 19-22. Also, as explained in the Order attached to the First Action, “*Solana* teaches the domain name service system uses ‘DNSsec’ to store a plurality of domain names and network addresses,” First Action (Order) at 6-7 (emphasis added), and that “a DNSsec directory service” is “an extension to the DNS.” First Action (Order) at 7.

In its Second Response, Patent Owner asserts that the “Office improperly asserts that *Solana* incorporates by reference *three different RFCs* allegedly disclosing these features based on *Solana*’s generalized reference to *one* of those RFCs *in a footnote*.” Second Response at 10. This challenge rests on two flawed premises; namely, (i) that a person of ordinary skill reading *Solana* would be unfamiliar with well-known industry standards that are being referenced in the *Solana* publication, and (ii) that to effectively reference well-known technologies, a printed publication must employ a particular style approved by the Office. Contrary to Patent Owner’s assertions, obviousness is assessed using a perspective of a person of ordinary skill in the art who is presumed to be familiar with widely used and well-known technologies in the field of the invention – in this case well-known Internet communication standards and technologies, such as DNS-sec. Patent Owner also challenges to the manner by which *Solana* references these technical descriptions. This challenge is grounded on a fundamental misunderstanding of the relevant law. Specifically, Patent Owner asserts that *Solana* is improperly “incorporating by reference” the three requests for comment discussed in the First Action and the Request (i.e., RFC 2065, RFC 1034 and RFC 1035). Patent Owner’s theory appears to be that a printed publication must formally incorporate other prior art disclosures using a particular form approved by the Office in order for a person of ordinary skill to be attributed knowledge in those prior art publications. There is no such requirement in the patent law. In *Harari v. Lee*, 656 F.3d 1331 (Fed. Cir. 2011), the Federal Circuit explained that “broad and unequivocal” language in a publication was sufficient to incorporate the full contents of the referenced prior art document. *Id.* at 1335. By making specific references to specific RFC documents describing well-known Internet networking technologies, *Solana* is directing the reader (a person of ordinary skill) in an

unequivocal and specific manner to the technical descriptions of these technologies (e.g., the DNS-sec protocol in RFC 2660, and the standards governing the well-known domain name server system within which the DNS-sec protocol functions described in RFC 1034 and RFC 1035). Similarly, the language used in *Solana* is “broad and unequivocal,” stating that “existing naming structures” such as “DNS-sec” may be used for the purpose of storing naming information in the DS.² And, of course, Patent Owner does not contend that a person of ordinary skill in the art would have any difficulty comprehending the teachings of *Solana*, or the publications describing these well-known Internet standards and technologies, such as DNS-sec. Finally, Patent Owner cannot seriously contend that the DNS-sec standard governed by RFC 2065 actually operates within the Internet’s standardized domain name service system (as documented in RFC’s 1034 and 1035). Patent Owner’s first challenge is thus meritless.

Patent Owner’s next challenge rests on its incorrect characterization of what *Solana* actually teaches to the person of ordinary skill in the art and what the claims specify. Patent Owner contends that *Solana*’s disclosure of DNS-sec “does not mean that *Solana*’s DS is necessarily configured to store domain names and corresponding network addresses, and to receive a query for a network address” even though *Solana* expressly states that “DNS-sec may be used for” the purpose of establishing a “coordinated, global Directory Service (DS) holding naming information and especially certificates that securely bind their domains to their public keys” within the *Solana* scheme. Second Response at 11.

Initially, Patent Owner did not advance this flawed and incorrect theory in its First Response. See Request at 42-44; First Action(Order) at 6-7. It should not now, in a belated manner, be permitted to do so. In any event, Patent Owner is wrong. As explained in the First Action, the DNS system of *Solana* expressly teaches use of “‘DNSsec’ to store a plurality of domain names and network addresses. Specifically, the UNI (comprising a domain name for secure services) corresponds to a network address and where the UNI and the network address are published (stored) in a directory service.” First Action (Order) at 7. The Office also explained that *Solana* discloses “receiving a query for a network address” because “a DNSsec directory service (an extension of the DNS) uses public keys and signatures to secure naming

² As noted by the Office, *Solana* specifically identifies DNS-sec in note 16. *Solana* at 50 (D.E. Eastlake. *Domain Name System Security Extensions*. Request for Comments 2065. January 1997). ACP at 19.

queries to a directory service (p. 39). One of ordinary skill in the art would recognize a name query to a DNS directory service would be to retrieve the above-mentioned network address.” First Action (Order) at 7. These conclusions of the Office and corresponding explanations in the Request were supported by Requester’s Expert Declaration. Comments at 5-9 (citing Fratto at ¶¶37-48). Thus, the Patent Office rejected the precise theory that Patent Owner now advances to incorrectly assert that the use of DNS-sec identified in *Solana* does not involve storage of domain names and corresponding addresses, or receiving a query for a network address. Because the Office was correct, the Office’s findings that the independent claims 1, 36 and 60 are anticipated by *Solana* was proper.

2. Dependent Claims 5, 23, and 47 (Issue Nos. 1, 2, 5, 6)

The Examiner correctly found that *Solana* discloses every limitation of dependent claims 5, 23, and 47. First Action at 5-7, 22. Specifically, the First Action and the Request explained that *Solana* shows that the source and destination domains in its system may be securely connected through an encrypted channel, which necessarily performs authentication and uses a cryptographic technique. *See, e.g.*, First Action at 5-7, 22; Request at 46, 52, 60-61, 66. In its First Response, Patent Owner did not contest these findings Office’s finding that *Solana* describes a DNS system that comprises a domain name service system that may be configured to authenticate a query for a network address, or that this can be done using a cryptographic technique. Now, in its Second Response, Patent Owner (incorrectly) contends that *Solana* does not teach what is specified by these dependent claims (i.e., that the “domain name service system is configured to authenticate the query [for a network address] using a cryptographic technique”).

Patent Owner should not be permitted to present these new arguments now, as they do not respond to issues set forth in the ACP. *See* 37 C.F.R. 1.951 (“the patent owner may once file comments limited to the issues raised in the Office action closing prosecution.”) (emphasis added). Indeed, Patent Owner admits that its new theory about *Solana* in connection with claims 5, 23 and 47 is not responsive to any issue raised by the Office in the ACP – it states that the “ACP provides no additional analysis of this feature, but instead incorporates by reference the proposed rejection from the Request.” Second Response at 12. A response under 37 C.F.R. 1.951 is not an opportunity for a Patent Owner to present new arguments; it must be limited to issues raised by the Office in the ACP.

As to the substance of its assertions, Patent Owner again mischaracterizes what *Solana* teaches and its relationship to the actual claim language, asserting that the claims require a precise sequence of steps to be performed to “authenticate the query using a cryptographic technique” that are not shown in *Solana*. Patent Owner is incorrect.

First, Patent Owner contends *Solana* does not anticipate claims 5, 23 and 47, arguing (incorrectly) that the encrypted channel described in *Solana* “has nothing to do with the alleged ‘query for a network address.’” Second Response at 12. This tortured reading of *Solana* is simply incorrect. *Solana* shows the secured channel is established in response to the initiator in the source domain issuing a query requiring interactions with the destination domain, which then triggers a sequence of authentication and encryption steps. The query is integral to this process of establishing the secure channel, and is described in more detail at pages 45-48 of *Solana*. Patent Owner also ignores that communications between principles and domains in the *Solana* systems necessarily involves queries sent between *different* domains – indeed one of stated purposes of the *Solana* schemes is to enable principles located in different domains to communicate securely, which requires secure communications to occur between domains.

Second, Patent Owner contends that the “communications between domains and principals is ... irrelevant here where the Office has asserted that the alleged request for a network address is received by *Solana*’s DS.” Patent Owner’s assertions rest on its mistaken belief that the *Solana* DNS systems will only “‘authenticate the query’ not *encrypt* it” and that “most of the portions cited by the Request” are *separate from and occur after* the alleged query for the network address is already answered.” Second Response at 11-12. *See also id.* at 12 (asserting that “most of the portions [of *Solana*] cited by the Request refer to *Solana*’s Figs 2a-3b, which ... are separate from and occur after the alleged query for the network address is already answered..”). Patent Owner is incorrect – *Solana* shows that information in the query is used at various stages of the *Solana* processes. *See, e.g., Solana* at pages 42-48.

Patent Owner’s flawed theories also rest on errors about what is actually claimed. For example, Patent Owner criticizes the *Solana* DNS systems, arguing they do not anticipate the claims because they consist of multiple components or because they do or do not perform specific steps in response to the content of a query. However, as explained in the Request and in the First Action, *Solana* shows that queries made within the *Solana* schemes, particularly in the DNS-sec embodiments of that scheme, are associated with establishment of the secure channel

(e.g., the destination specified in the request triggers a sequence of steps resulting in authentication and establishment of the secure channel between the origination domain and the destination domain). More importantly, Patent Owner's arguments all rest on the assumption that its claims imposes requirements or restrictions about the sequence of steps that must be performed before, during or after the query. They do not – the claims specify simply "... a domain name service system configured ... to receive a query for a network address..." and that a "*domain name system* is configured to authenticate the query using a cryptographic technique." '504 patent at claims 1, 5 and 23 (emphasis added). *Solana* anticipates these claims because it shows that queries may be authenticated using certificates and keys (i.e., each of which involves use of "a cryptographic technique"). The putative distinctions Patent Owner points to relative to the *Solana* systems, thus, are not actually claimed. Under its well established policies and practices, the Office may not incorporate these various and varying limitations into the claims absent a change to the language of these claims. The Office's rejection of claims 5, 23 and 47 as being anticipated by *Solana* was thus proper and should be maintained.

3. Dependent Claims 8 and 9 (Ground Nos. 1, 5)

The Office correctly found that *Solana* discloses a domain name service that is connected to a virtual private network established between two domains. ACP at 23. Patent Owner disagrees, asserting, as it did after the First Action, that somehow the indication in *Solana* that "organizations concerned by security issues . . . interact with the Internet . . . by means of well-protected Virtual Private Networks (VPN)" does not show that the DNS system of *Solana* satisfies these claim requirements. Second Response at 13-14. Patent Owner is simply incorrect. As explained in the ACP, this disclosure in *Solana* "is not a suggestion." ACP at 23. Moreover, Patent Owner fails to consider the teachings of *Solana* as a whole. As explained in Requester's Comments, *Solana* indisputably discusses the interplay of its system with VPNs. In particular, in discussing how its systems manage inter-domain confidentiality, *Solana* explains:

The functionality offered by the DBSs in this scheme is often known as *secure gatewaying*. The main advantage of inter-domain confidentiality lies in the fact that services may be provided *transparently* to the parties involved in the transaction. This is especially convenient for:

- Organizations having well protected private networks which are mostly concerned by securing bulk data exchanges beyond their borders at low management costs.

Solana at 45 (emphasis added); *see* Comments at 10. This explanation (which Patent Owner ignores) shows that the *Solana* DNS systems interface with and support communications over “private networks” (i.e., VPNs), and are thus “connectable” to VPNs. Consequently, the Office’s rejection of claims 8 and 9 as anticipated by *Solana* was proper.

4. Dependent Claims 16, 17, 27, 33, 40, 41, 51, and 57 (Ground Nos. 1, 5)

The Office correctly found that *Solana* discloses every limitation of dependent claims 16, 17, 27, 33, 40, 41, 51, and 57. ACP at 22. In response, Patent Owner presents no distinct basis for asserting that claims 16, 17, 27, 33, 40, 41, 51 and 57 are not anticipated by *Solana* relative to the arguments it presents regarding anticipation of claims 1, 36 and 60 by *Solana*. Given that the Office’s rejection of claims 1, 36 and 60 was proper, its rejection of these dependent claims as anticipated by *Solana* also was proper.

5. Dependent Claims 18 and 42 (Ground Nos. 1, 5).

The Office correctly found that *Solana* discloses every limitation of dependent claims 18 and 42, including that “at least one of the plurality of domain names is reserved for secure communication links.” In response, Patent Owner asserts “the Office eviscerates the meaning of the claim language by asserting that the domain names that are allegedly ‘reserved’ for secure communications links need not be used for secure communication links.” Second Response at 14. Patent Owner misrepresents the Office’s findings and ignores the actual claim language. The Office explained that, in certain circumstances explained in *Solana*, a “domain name is reserved for secure communication links.” ACP at 23-24. The Office explained that nothing in the claim requires that “the initiator . . . take advantage of the reservation.” ACP at 23-24. Patent Owner again seeks to distinguish *Solana* using unclaimed limitations in claims 18 and 42 (e.g., that the “reserved” domain names must actually be used only for secure communication links). Consequently, the Office’s rejections of claims 18 and 42 as anticipated by *Solana* were proper.

6. Dependent Claims 24 and 48 (Ground Nos. 1, 2, 5, 6).

The Office correctly found that *Solana* discloses every limitation of dependent claims 24 and 48, including the requirement that “at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link.” For example, in the First Action, the Office correctly determined that *Solana* teaches the functional correlation between a secure domain name (e.g., that it is associated with a certificate)

and establishing a secure communication to that domain. In response, Patent Owner asserted that while “*Solana* discloses domain names that are associated with certificates needed for secure transactions,” “those domain names are not ‘secure names’ associated with secure communications” within the meaning of claim 24. See First Response at 24. Patent Owner’s theory why this is the case is that “just because a domain name is associated with a certificate does not mean that the domain name itself comprises an indication that a domain name system supports establishing a secure communication link.” First Response at 48. Patent Owner, thus, asserted that the domain name itself (e.g., an arbitrary string of characters) is what distinguishes claims 24 and 48 from the prior art systems shown in *Solana*. The Office correctly rejected this assertion, explaining that the value of the domain name itself is non-functional information incapable of distinguishing the claims from *Solana*. As the Office stated, “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” and is thus 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.” ACP at 24.

Now, in its second response, Patent Owner seeks to backtrack on its arguments in the First Response, asserting that claims 24 and 48 specify “a functional relationship between the ‘at least one of the plurality of domain names’ and the ‘domain name service system.’” (emphasis added) Second Response at 15. In other words, in its First Response, Patent Owner asserted that the value of the domain name itself was the important distinction over the *Solana* systems, but now asserts there is a “functional” relationship between the “domain name” and the DNS system is required. Patent Owner’s vacillations demonstrate the Office is correct to reject the claims. As explained in the First Action, *Solana* shows DNS systems comprising a functional relationship between a domain name and that system, including through use of a particular certificate associated with a secure domain which is used by the DNS system to authenticate and establish a secure communications link to that secure domain. The distinction Patent Owner attempts to make now – that the “domain name” provides a functional role of an “indication” that the domain is a secure one – fails to distinguish the claims from *Solana*.

Indeed, the precise analogy used by Patent Owner in the Second Response (i.e., “indicia on a measuring cup that indicate that the measure cup stores a particular volume”) shows the

Office is correct. The claims permit a certificate associated with a domain name or the domain name itself to serve the functional role of identifying the secure domain. In Patent Owner's measuring cup example, markings on the measuring cup – whether printed, scored into the glass, or otherwise represented -- serve the identical functional role of indicating volume. Consequently, the Office's rejections of 24 and 48 claims as anticipated by *Solana* was proper.

7. Dependent Claims 26 and 50 (Ground Nos. 1, 5).

The Office correctly found that *Solana* discloses every limitation of dependent claims 26 and 50, including that “at least one of the plurality of domain names enables establishment of a secure communication link.” Patent Owner disagrees, re-arguing that “DNS-sec” was not properly incorporated by reference in *Solana*. Second Response at 17. As explained above, Patent Owner is incorrect. The only other argument Patent Owner advances—that “merely returning an address and public key based on a DNS query does not disclose that the domain name . . . enables anything”—is the same argument it made in its First Response, which has already been rejected by the Office. ACP at 25. Consequently, the Office's rejection of claims 26 and 50 as anticipated by *Solana* was proper.

8. Dependent Claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59 (Ground Nos. 1-8).

The Office correctly found that *Solana* discloses every limitation of dependent claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59. Patent Owner does not specifically contest any of these findings, but instead refers to its arguments regarding independent claims 1 or 36. Because claims 1 and 36 were properly rejected, these dependent claims also were properly rejected. Consequently, the Office's rejection of claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59 as anticipated by *Solana* was proper.

B. Rejection of Claims 2-5, 24, 25, 37, 48 and 49 Based on *Solana* in view of RFC 920 (Issue No. 2)

Patent Owner does not specifically contest any of the findings of the Office in the ACP based on *Solana* in view of RFC 920, but simply relies on its positions stated with respect to *Solana* alone. Consequently, the rejection of claims 2-5, 24, 25, 37, 48 and 49 as set forth in the ACP as being obvious based on *Solana* in view of RFC 920 was proper.

C. Rejection of Claims 10-13 Based on *Solana* in view of *Reed*, or *Solana* in view of RFC 2504 and *Reed* (Issue No. 7)

The Office rejected claims 10-13 in the First Action over *Solana*, considered in view of *Reed* or in view of RFC 2504 and *Reed*. See First Action at 5; First Response at 36. The only basis Patent Owner presented in its First Response to these rejections was that *Reed* was not proven to be prior art. The Office did not find this argument persuasive. Now, in its Second Response, Patent Owner belatedly contests the substantive findings set forth in the First Action regarding *Reed*, contrary to 37 C.F.R. 1.951.

Patent Owner also presents a flawed and inaccurate description of what *Reed* teaches, and uses this flawed description of *Reed* to challenge the actual rejection. Patent Owner appears to recognize that, in the First Action, the Office explained that *Reed* showed a method that “‘pseudorandomly’ changes IP addresses because it routes the IP traffic according to schemes that appear [] random, but are in fact pre-defined.” Second Response at 18. However, Patent Owner somehow concludes that the “onion” in the *Reed* scheme is the claimed data packet, and that “*Reed* does not disclose inserting into each alleged data packet (i.e., the onion) one or more data values that vary according to the pseudo-random sequence, as claimed.” *Id.* What *Reed* actually shows is that its onion-routing scheme is implemented by routing IP packets through pre-defined onion routers using the IP addresses of those routers. Thus, *Reed* teaches a scheme as defined in dependent claim 10, and the Office properly found claims 10 (and claim 11, for which Patent Owner presents no response) obvious based on *Solana* in view of *Reed*.

Patent Owner makes similar errors with respect to claim 12. Here, Patent Owner seeks to distinguish the limitation “comparing a value in each data packet transmitted between a first device and a second device to a moving window of valid value.” The Office and the Requester explained that the procedures in *Reed* meet this requirement because sets of IP addresses corresponding to the different addresses of different onion routers are used in a varying manner in the *Reed* onion routing scheme. See Request at 84-86; First Action at 5. Once again, Patent Owner seeks to distinguish *Reed* by resort to unclaimed limitations of the claims that would limit how this claim requirement is met, and by mischaracterizing what is shown in *Reed*. Because the rejections of claims 10 and 12 based on *Solana* in view of *Reed*, and based on *Solana* in view of RFC 2504 and further in view of *Reed*, were proper, they should be maintained. Requester also notes Patent Owner provides no response regarding claims 11 and 13, and rejections of these claims thus should be maintained.

D. Rejection of Claims 7, 32, and 56 Based on *Solana* in view of *Beser* (Issue No. 4)

Patent Owner presents no response to the rejection of claims 7, 32 and 56 that is distinct from its response to claims 1 and 36, and makes no observations about the combined teachings of *Solana* and *Beser*. Because the rejection of claims 1 and 36 was proper, the Office's rejection of claims 7, 32 and 56 claims as obvious based on *Solana* in view of *Beser* was also proper.

E. Rejection of Claims 1, 2, 5, 6, 8, 9, and 14-60 Based on *Solana* in view of RFC 2504 (Issue No. 5)

Patent Owner does not contest any of the evidence or explanations in the ACP supporting the rejection of the recited claims based on *Solana* in view of RFC 2504. Instead, Patent Owner simply references its original response to the First Action. In the ACP, the Office correctly found Patent Owner's original response unpersuasive. Consequently, the Office's rejection of these claims as obvious based on *Solana* in view of RFC 2504 was proper.

F. Rejection of Claims 2-5, 24, 25, 37, 48, and 49 Based on *Solana* in view of RFC 2504 and RFC 920 (Issue No. 6)

Patent Owner does not contest any of the evidence or explanations in the ACP specific to *Solana* in view of RFC 2504 and RFC 920, but instead relies on its positions with respect to *Solana*, RFC 2504 and RFC 920 individually. Consequently, the Office's rejection of these claims as obvious based on *Solana* in view of RFC 2504 and RFC 920 was proper.

G. Rejection of Claims 7, 32, and 56 Based on *Solana* in view of RFC 2504 and *Beser* (Issue No. 4)

Patent Owner does not contest any of the evidence or explanations in the ACP that are specific to *Solana* in view of RFC 2504 and *Beser*, but instead relies on its positions stated with respect to *Solana*, RFC 2504 or *Beser* alone. Consequently, the Office's rejection of these claims as obvious based on *Solana* in view of RFC 2504 and *Beser* was proper.

IV. Rejection of Claims 1-2, 5-6, 8-9, and 14-60 Under 35 U.S.C. § 102(b) based on *Provino* (Issue No. 9).

A. Response Concerning Independent Claims 1, 36, and 60

As explained in the Request and confirmed by the Office, *Provino* describes secure DNS systems and methods for establishing secure communication links between devices connected to public networks, such as the Internet. Request at 119-20; First Action at 8-10. The *Provino* DNS systems comprise not only a first name server 17 located outside the secure network, but

also a device 12(m), a firewall 30, and a secure name server 32 residing behind the firewall. See *Provino* at Fig. 1. These components work together in a coordinated manner to evaluate requests to establish secure connections, direct network traffic via firewall 30 and secure name server 32 to secure destinations, perform authentication and encryption of traffic and other functions needed to establish and maintain secure communication links. Request at 117-66; First Action at 8-10. See also *Provino* at 2:66 to 3:22 (describing its system as “comprising a virtual private network and an external device interconnected by a digital network”). Consequently, the Office properly found that *Provino* anticipates independent claims 1, 36 and 60.

In its Second Response, Patent Owner presents a new set of theories why it believes *Provino* does not anticipate claims 1, 36 and 60, none of which were advanced in its First Response. First, Patent Owner contends that *Provino*'s VPN firewall 30 is not a DNS system component, and thus, the *Provino* DNS systems that include this component do not anticipate claims 1, 36 and 60. Second, Patent Owner contests the Office's findings that various aspects of *Provino*'s DNS systems provide “indications” within the meaning of these claims. Here, Patent Owner challenges both the Office's determination as to what may constitute an indication, as well as the Office's description features in the *Provino* DNS systems that comprise these indications (e.g., that the establishment of a secure tunnel in *Provino* between the external device 12(m) and the firewall 30 does not comprise the claimed “indication”, that firewall 30 providing the device 12(m) with the identification of VPN name server 32 does not comprise the claimed “indication” and that name server 17 does not comprise the claimed “indication.”). Second Response at 26-30. Each assertion rests on Patent Owner's flawed reading of the claims and incorrect description of what *Provino* discloses.

1. *Provino*'s “Firewall 30” is Plainly a Functional Component of the *Provino* DNS Systems

As explained in the First Action and the Request, the *Provino* DNS systems comprise not only a first name server 17 located outside the secure network, but also a device 12(m), a firewall 30, and a secure name server 32 residing behind the firewall. See, e.g., First Action at 8-9; Request at 117-22; *Provino* at Fig. 1; *id.* at 2:66-3:23. These components in *Provino* work together in a coordinated manner to evaluate requests to establish secure connections, direct network traffic via firewall 30 and secure name server 32 to secure destinations, perform

authentication and encryption of traffic and other functions needed to establish and maintain secure communication links. See First Action at 9; Request at 117-66.

In the First Response, Patent Owner focused on name server 17 in isolation, contending that this one component did not provide an “indication” specified in the claims. First Response at 19-21. In the ACP, the Office pointed out the Patent Owner’s serious error. See ACP at 26 (“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.”). Indeed, how Patent Owner came to believe that the rejections over *Provino* were based on name server 17 in isolation is a mystery – the Office and the Request both clearly explained that *Provino* disclosed DNS systems that provided the claimed “indication” without making any reference to name server 17. First Action at 9-10 (“[T]he VPN Name [Server] 32 will provide the requested network address in a message packet to the firewall 30, where the firewall then transmits the address to device 12(m) in encrypted within a secure VPN tunnel, which provides an indication that the DNS system supports establishing a secure link.”) (emphasis added) Moreover, in the First Action, the Office plainly identified firewall 17 as being simply one component of the *Provino* DNS systems, and clearly explained why the *Provino* DNS systems including this component anticipated the claims. The Office did not change its position between the First Action and ACP – it maintained in both that the *Provino* DNS systems – not an individual component of them – anticipate the claimed systems.

Against this backdrop, Patent Owner now contends the Office has “unreasonably expanded its interpretation of DNS system with respect to *Provino*” and that this had caused confusion in the mind of the Patent Owner about why *Provino* anticipates claims 1, 36 and 60. Second Response at 22. Any confusion Patent Owner is experiencing now is the result of its studied ignorance of the First Action, the Request, and the *Provino* disclosure. More remarkably, Patent Owner now challenges the rejections by focusing on firewall 30 in isolation. Like its peculiar focus on nameserver 17 in its First Response, this response based on firewall 30 in isolation is misplaced and irrelevant.

Initially, Patent Owner could have raised new theories about firewall 30 not being part of the *Provino* systems in its Response to the First Action. As noted above, the First Action and the Request each plainly identified firewall 30 as part of the *Provino* DNS systems that anticipated claims 1, 36 and 60. Patent Owner did not, and instead elected to present its new “firewall 30”

theory only after the ACP issued in this case. Consequently, Patent Owner should be precluded from raising these new arguments at this stage of the proceeding.

Patent Owner's new theories are also plainly incorrect based on what *Provino* teaches. For example, Patent Owner contends that "firewall 30" cannot be a component in *Provino*'s DNS system because it "has no DNS-related functionality." Second Response at 23. Patent Owner's "DNS-functionality" theory is irrelevant to the analysis of whether the claimed DNS systems are anticipated by *Provino* – the claims contain no language in them defining what components must be included or excluded from the claimed DNS systems, much less specify some "DNS functionality" requirement for each of the components in these DNS systems. Instead, the claims simply specify that the DNS systems provide the functionality specified in the claims. Moreover, "firewall 30" is plainly described in *Provino* as being a functional component of the *Provino*'s DNS systems. Indeed, Patent Owner describes its own DNS systems in the '504 patent in a manner highly analogous to how *Provino* describes its DNS systems. For example, *Provino* explains that firewall 30 and the other components in its DNS systems play an interrelated and interdependent role in the establishment of a secure communication link in response to a request for a controlled ("internal") resource. *Provino* at 2:66-3:23. In an analogous manner, the '504 disclosure identifies traversing a firewall as being part of its system "for establishing a virtual private connection that is encapsulated using an existing network protocol." See '504 Patent at 9:35-37 (describing Fig. 37); *id.* at 55:31-43. Patent Owner's new argument that "firewall 30" is not part of the *Provino* DNS system because it has no "DNS-related functionality" is thus both factually incorrect and legally irrelevant.

Patent Owner next asserts that "firewall 30" cannot be a component in *Provino*'s DNS system because "*Provino* does not disclose any interaction between it and the other alleged components of the DNS system." This is plainly false for reasons presented in the First Action (and the Request) (i.e., "the VPN Name [Server] 32 will provide the requested network address 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.") First Action at 9. Moreover, the fact that a firewall can act on network traffic other than that which originates from the name server 17 component of *Provino* is irrelevant – in the systems described in *Provino*, firewall 30 functions integrally with the other components of the *Provino* DNS systems to convey requests requiring resolution by the secure domain name server 32. ACP at 26-29. Thus, Patent Owner is thus

simply incorrect in describing what *Provino* actually teaches about firewall 30 and its relationship to the other components of the *Provino* DNS systems.

Patent Owner also asserts that because it “criticizes” or “disparages” prior art firewalls, *Provino*’s firewall 30 cannot be considered to be a component of the claimed DNS systems. This theory borders on the frivolous. As explained above, it is the words of the claims that determine whether a claim is anticipated, not some vaguely expressed description of the prior art by the patent owner in its patent disclosure. Because the language used in claims 1, 36 and 60, causes them to encompass the *Provino* DNS systems, each of these claims is anticipated by these prior art DNS systems. Moreover, even if Patent Owner’s “disclaimer” theory were relevant in practice before the Office (which it is not), there is nothing in the ’504 disclosure that actually disclaims the *Provino* DNS systems, or the manner in which the components in the *Provino* DNS systems (including firewall 30) are actually used. Instead, Patent Owner’s vague language in the ’504 patent “disparaging” prior art firewalls in no way concerns how firewall 30 is specifically used within the *Provino* DNS systems. Moreover, because the claims do not include any limitations that actually exclude from their scope the *Provino* DNS systems that include firewall 30, this observation by Patent Owner is simply irrelevant and must be ignored. The Office correctly found claims 1, 36 and 60 anticipated by the *Provino* DNS systems.

2. *Provino* Teaches DNS Systems that Comprise an “Indication” Specified in Claims 1, 36 and 60

The Office correctly found that *Provino* discloses DNS systems configured to “comprise an indication that the domain name service system supports establishing a secure communication link” (and corresponding provisions in claims 36 and 60). First Action at 8-10; ACP at 25-29. In addition, the Office noted that Patent Owner’s First Response “incorrectly focus[es] on name server 17 . . . without addressing the role of the firewall 30 and VPN name server 32.” ACP at 26. In its Second Response, Patent Owner now contests this determination for the first time. As these comments do not address issues raised in the ACP, they should not be admitted pursuant to 37 C.F.R. 1.951.

Patent Owner also levies several criticisms of the Office’s determination that *Provino* discloses an “indication” within the meaning of claims 1, 36 and 60. The first of these asserts that the Office has changed its position relative to the First Action, and that it now contends that an “indication” is “a visible message or signal to a user that the DNS system supports

establishing a secure communication link.” Second Response at 26. Patent Owner then complains that the Office, after supposedly making this finding, did not “apply its claim construction to these alleged ‘indications’ in *Provino*.” *Id.*

Patent Owner’s confused remarks should be ignored. The Office clearly explained in the First Action and in the ACP why the *Provino* DNS systems comprise “indications” within the meaning of the claims. The Office’s held that the term “indication” read in its broadest reasonable construction could encompass many types of indications, and is not limited to any one those reasonable meanings. It then observed – in response to Patent Owner’s assertions in the First Response – that an “indication” could be one that is visible to a user. ACP at 25-26. Patent Owner’s “confusion” is of its own making – the Office’s position on the broadest reasonable construction of “indication” were clearly explained, and consistently followed and applied in the First Action and the ACP, and its finding that this claim term is met by three different aspects of the *Provino* DNS systems is correct.

Patent Owner next presents challenges to the three examples of indications disclosed in *Provino*. Each is based on a contorted and inaccurate reading of *Provino* and ignores the actual claim language. Each is thus incorrect.

First, Patent Owner contends, after reiterating its flawed theory that firewall 30 is not part of the *Provino* DNS systems, that an indication must be a “visible message or signal to a user,” and that the Office’s finding that the establishment of a secure tunnel in *Provino* constitutes an “indication” is therefore inconsistent with the claim language. Second Response at 27. Again, Patent Owner misreads the claims. The clause quoted by the Patent Owner does not refer to two different acts – it reads simply “an indication that the domain name service system supports establishing a secure communication link.” The claims, read in their broadest reasonable construction, thus do not preclude a finding that establishment of a secure communications link provides the claimed indication. This clearly is not situation where a claim expressly specifies two different components on an apparatus, and the prior art shows only one of those components. Patent Owner’s reliance on M.P.E.P. § 2131 thus is misplaced.

Next, Patent Owner contests the Office’s determination that the provision of the secure name server 32 to device 12(m) within the *Provino* DNS systems constitutes an “indication.” Here, Patent Owner raises two new theories for the first time. First, it contends “the firewall 30 merely identifying the name server 32 to the device 12(m) indicates nothing of the actual

capabilities of the name server 32, much less whether it has the capacity to establish a secure communication link.” Second Response at 28. This simply mischaracterizes the *Provino* teachings. The identification of secure name server 32 to device 12(m) plainly does convey an indication that the DNS system supports establishing secure communication links, as this is the sole function of these aspects of the *Provino* systems. Second, Patent Owner contends that firewall 30 establishes the secure tunnel without any assistance from the VPN name server, and thus “one of ordinary skill would not view *Provino*’s firewall 30 as capable of indicating that name server 32 supports establishing a the secure communication link.” This contorted reading of *Provino* borders on the absurd. The secure communication link being discussed in *Provino* necessarily involves interactions with between firewall 30 and secure name server 32 to establish the secure connection to the internal network resource which is identified by name server 32. Fratto at ¶53. Patent Owner’s theory that only firewall 30 is involved in establishing the secure tunnel is thus both wrong and irrelevant. Again, Patent Owner mistakenly attacks a single component in the *Provino* systems (firewall 30), asserting that this component in isolation does not perform all of the functions of the claimed DNS systems. Patent Owner’s flawed reading of how the *Provino* DNS systems function, coupled to its flawed understanding of what its claims encompass, should simply be ignored.

Finally, Patent Owner asserts the Office’s determination that *Provino* name server 17 provides an “indication” within the meaning of the claims was misplaced, arguing that name server 17 (which it portrays as being a conventional name server) “does nothing whatsoever to support establishing a secure communication link or indicate it supports establishing one...” Second Response at 29. Once again, instead of challenging what the Office actually found (i.e., that name server 17 operating in conjunction with firewall 30 and secure name server 32 provides the specified indication), Patent Owner challenges its own distorted and inaccurate depiction of the Office’s findings. As was explained in the Request and the First Action, name server 17 serves a particular functional role within the *Provino* DNS systems – it identifies, in response to a particular type of request, the address of the firewall 30, which enables that request to be routed to the secure nameserver 32. Request at 117-22. Patent Owner takes issue with this characterization of *Provino* for the first time in its Second Response, asserting various theories why this does not constitute the claimed “indication.” All of these incorrect assertions can be simply ignored because they are predicated on Patent Owner’s belief that the claims incorporate

specific requirements regarding the “indication” which are not actually recited in the language of the claims. Patent Owner also again asks the Office to treat its “disclaimer” of conventional firewalls as an effective claim limitation that excludes what the language used the claims actually encompasses. *See* Second Response at 29-30 (“...name server 17 does nothing beyond mechanically returning an address that corresponds to a domain name, which is a conventional DNS feature disclaimed by the ’504 patent...”). Without adding language to its claims to exclude the embodiment of an “indication” shown in *Provino*, Patent Owner’s assertions are ineffective in this proceeding, and must be ignored.

Consequently, the Office correctly found that *Provino* anticipates every element of independent claims 1, 36 and 60, and the rejections of these claims should be maintained.

B. Response Concerning Dependent Claims 5, 23, and 47

The Examiner correctly found that *Provino* discloses every limitation of dependent claims 5, 23, and 47. First Action at 7; ACP at 8, 29-30. In response, Patent Owner claims the Office is improperly “clarify[ing] its position” in the ACP. Second Response at 30-31. Patent Owner then contests the Office’s findings for three different reasons.

First, Patent Owner asserts that “firewall 30” is not a component of *Provino*’s DNS system. As explained above, this assertion is simply wrong – the *Provino* DNS systems comprise firewall 30 acting in conjunction with nameserver 17, device 12(m) and nameserver 32. Request at 117-22; ACP at 27.

Second, Patent Owner asserts that “authorization” and “authentication” have precise and distinct meanings to a person of ordinary skill in the art. Again, Patent Owner is wrong – neither term is defined in the ’504 specification to have a particular, fixed meaning, and neither term has a uniform or unique meaning established in the prior art. Instead, Patent Owner seeks to again improperly import a substantive limitation into the claims, this time via its expert’s general assertions about the relative meanings of the terms “authentication” and “authorization.” Patent Owner’s hand-waving about its claims cannot distinguish them from the *Provino* disclosure. Instead, Patent Owner must actually amend the claims if it wishes them to require performance of a particular sequence of steps (and to exclude other steps). This, of course, would also require Patent Owner to demonstrate written description support for these new claims. Without doing so, Patent Owner’s arguments must be disregarded.

Finally, Patent Owner incorrectly contends that the Office improperly relied on different “queries” that occur in the *Provino* DNS systems to find claims 5, 23, and 47 anticipated. Again, Patent Owner mischaracterizes what *Provino* actually shows, and then asserts its claims require something, which, by their actual terms, they do not. Patent Owner first criticizes the Office’s reliance on “one” authenticated query occurs with the request to establish a secure tunnel, and its reliance on a “totally different” authenticated query that occurs when an authenticated query for a network address is sent to name server 32. Patent Owner’s putative distinctions are illusory – each authenticated query (which Patent Owner now acknowledges does occur in the *Provino* DNS systems) is unquestionably part of the same sequence that results in establishment of the secure tunnel. Moreover, rejected claims specify simply a DNS system configured “to authenticate the query using a cryptographic technique” (claim 5) or “to authenticate the query for the network address” (claim 23, 47). They do not, as Patent Owner contends, specify when authentication must occur (e.g., before vs. after “firewall 30 receives the request to establish a secure tunnel”). Moreover, the claims do not foreclose authentication steps being performed multiple times during the process of establishing a secure tunnel. *See* Requester Comments at 16. The Office also noted in its ACP that the claims place no limitations on when the authentication must be performed, such that the claimed “authentical[ion] . . . using a cryptographic technique” described in ’504 may be performed in the *Provino* system after the query is received at firewall 30 and prior to the related query being sent to nameserver 32. Thus, based on Patent Owner’s own admissions, *Provino* shows a DNS system configured to “authenticate a query” as the claims specify, and therefore anticipates these claim. The Office’s rejection of claims 5, 23 and 47 as being anticipated by *Provino* thus was proper.

C. Response Concerning Dependent Claims 8 and 9 (Ground Nos. 1, 5)

The Office correctly found that *Provino* discloses a domain name service connectable to a virtual private network. ACP at 30. Patent Owner disagrees, contending that the Office never attempts “to explain how the alleged DNS system in *Provino*, under its new (but unreasonably broad and incorrect) construction, allegedly remains connectable to a virtual private network...” Second Response at 32. Patent Owner is simply incorrect. The First Action incorporated the Request, which describes in detail how *Provino*’s DNS system is “connectable to a virtual private network.” Request at 124. Moreover, as explained above, the Office’s construction of “DNS system” is neither “new” nor “unreasonably broad and incorrect.” Rather, it was Patent

Owner who elected to not address the explanations in the Request and incorporated in the First Action establishing that *Provino* meets the limitations of claims 8 and 9. *See* Request at 124, First Action at 7. Instead, Patent Owner asserted (incorrectly) that the rejection rested on the assumption that name server 17 constituted the entirety of the *Provino* DNS system. First Response at 38.

Patent Owner's new theory, advanced for the first time in its Second Response, should be excluded from consideration because it attempts to belatedly respond to an issue raised in the First Action. This new theory also can be dismissed because it is simply illogical and has no relationship to what is actually claimed. Specifically, Patent Owner now contends that because "firewall 30 and name server 32 are *part* of the VPN 15" they are "not connectable to it." This absurd theory ignores how the *Provino* actually work – the DNS system components perform steps that establish (and thus connect to) a VPN. Moreover, neither the claims nor the patent attach any special meaning to the word "connectable" that would foreclose the Office's conclusion that the interactions that occur between name server 17, device 12(m), firewall 30, and/or name server 32 constitute a DNS system "connectable with a VPN." Consequently, the Office's rejection of claims 8 and 9 as anticipated by *Provino* was proper.

D. Response Concerning Dependent Claims 24 and 48 (Ground Nos. 1, 2, 5, 6).

The Office correctly found that *Provino* discloses every limitation of dependent claims 24 and 48, including the requirement that "at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." ACP at 30-31. In response, Patent Owner asserted that the value (rather than the functional role) of the domain name alone was why claims 24 and 48 were distinct from *Provino*. In response, the Office explained that this distinction was ineffective to overcome the rejection, as the domain name itself constitutes non-functional descriptive material that cannot distinguish a claim from the prior art. Consequently, the Office correctly maintained the rejection. Now, as it did with respect to the rejection of claims 24 and 48 over *Solana*, Patent Owner changes its position, and contends there is a "functional relationship" between the domain name and the secure communication link. However, rather than describe how this allegedly functional relationship distinguishes claims 24 and 48 from the *Provino* systems, Patent Owner simply refers the Office to its response to the rejection of claims 24 and 48 over *Solana*. Since those reasons were unpersuasive, they also do not overcome the rejections based on *Provino*.

Consequently, the Office was correct in finding claims 24 and 48 anticipated by *Provino*, and the rejection of claims 24 and 48 as anticipated by *Provino* was proper.

E. Response Concerning Dependent Claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59

The Office correctly found that *Provino* anticipates dependent claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59. ACP at 8. Patent Owner presents no response specific to the rejections of these claims, but simply refers to its response to the rejection of claims 1 and 36 over *Provino*. Patent Owner thus concedes that these claims are not patentably distinct from claims 1 and 36. Moreover, because the rejection of claims 1 and 36 was proper, the rejection of these claims should also be maintained.

F. Rejection of Claims 2-5, 24, 25, 37, 48 and 49 Based on *Provino* in view of RFC 920 (Issue No. 10)

The Office correctly found claims 2-5, 24, 25, 37, 48 and 49 obvious based on *Provino* in view of RFC 920. The Patent Owner presents no response to the specific findings supporting the rejection for obviousness. Instead, Patent Owner simply contests that *Provino* and RFC 920 considered individually anticipate the claims. Consequently, because no contrary evidence has been advanced to rebut these findings, the rejection of these claims was proper.

G. Rejection of Claims 10-13 Based on *Provino* in view of *Reed* (Issue No. 11)

The Office rejected claims 10-13 in the First Action based on *Provino* in view of *Reed*. First Action at 5. The only challenge Patent Owner made to this rejection in its First Response was that *Reed* was not prior art to the claims. First Response at 5-8. Because this was incorrect, the Office correctly maintained the rejection for obviousness. Now, in its Second Response, Patent Owner contests the Office's findings concerning *Reed* set forth in the First Action. Again, Patent Owner's belated response is contrary to Rule 1.951. Patent Owner's new assertions are also incorrect. Here, Patent Owner simply repeats its flawed analysis of *Reed* first presented in its response to rejections based on *Solana* in view of *Reed*. See § II.C. Because Patent Owner mischaracterized there how the *Reed* onion routing schemes actually work, and ignored what rejected claims actually specify, its response here is also unpersuasive. See § II.C. Requester also notes that Patent Owner provides no response concerning claims 11 and 13, and thus does not contest these rejections. The rejection of claims 10-13, accordingly, should be maintained.

H. Rejection of Claims 7, 29-32, and 53-56 Based on *Provino* in view of *Beser* (Issue No. 12)

The Office correctly found claims 7, 29-32 and 53-56 obvious based on *Provino* in view of *Beser*. Patent Owner does not contest any of specific findings set forth in the Request and adopted by the Office relating to the obviousness of the claims. Instead, it simply contests that *Provino* and *Beser* considered individually anticipate the claims. As no response to the factual findings relating to obviousness was provided, Patent Owner has no basis for contesting that claims 7, 29-32 and 53-56 are obvious over *Provino* in view of *Beser*. Consequently, the rejection for obviousness of these claims should be maintained.

I. Rejection of Claims 1, 2, 5, 6, 8, 9 and 14-60 Based on *Provino* in view of RFC 2230 (Issue No. 13)

The Office correctly found claims 1, 2, 5, 6, 8, 9 and 14-60 obvious based on *Provino* in view of RFC 2230. Patent Owner does not contest any of the specific findings set forth in the Request and adopted by the Office relating to the obviousness of the claims. Instead, Patent Owner simply states “RFC 2230 does not make up for the deficiencies of *Provino* discussed above with respect to dependent claims 5, 8, 9, 23, 24, 47 and 48 for at least the reasons below [responding to rejections for anticipation by RFC 2230].” Because Patent Owner presents no response specific to the findings of obviousness of these claims, it has no basis for contesting that the rejection of these claims based on *Provino* in view of RFC 2230 was proper.

J. Rejection of Claims 2-5, 24, 25, 37, 48 and 49 Based on *Provino* in view of RFC 2230, in further view of RFC 920 (Issue No. 14)

The Office correctly found claims 2-5, 24, 25, 37, 48 and 49 obvious based on *Provino* in view of RFC 2230, and further in view of RFC 920. In response, Patent Owner asserts simply that the rejected claims depend from independent claims 1 and 36, and that “RFC 920 does not make up for the above-noted deficiencies of *Provino* and RFC 2230 discussed above concerning the rejection of these claims.” Second Response at 35. As no response is provided to the specific findings of the Office concerning obviousness was presented by Patent Owner, it has no basis for contesting that the cited claims would have been obvious based on *Provino* in view of RFC 2230, and further in view of RFC 920, and the rejection should be maintained.

K. The Rejection of Claims 10-13 Based on *Provino* in view of RFC 2230, and in further view of *Reed* (Issue No. 15) Was Proper

Patent Owner's response to this rejection is essentially identical to its response to the rejection of these claims based on *Provino* alone in view of *Reed*. Because that response rests on an incorrect description of what *Reed* actually describes and teaches, and fails to present any response specific to the combined teachings of *Provino* and RFC 2230, considered with *Reed*, Patent Owner's response should be disregarded and the rejection maintained.

L. The Rejection of Claims 7, 29-32, and 53-56 Based on *Provino* in view of RFC 2230, and in further view of *Beser* (Issue No. 16) Was Proper

Patent Owner presents no response to the specific findings in the Request and adopted by the Office as to why claims 7, 32 and 56 are obvious based on *Provino* in view of RFC 2230 and further in view of *Beser*. Instead, it simply asserts claims 1 and 36 are not anticipated by *Provino*, and refers to comments it made in three other sections of its Second Response. Second Response at 35-36. Patent Owner thus presents no specific response to the rejection of claims 7, 29-32 and 53-56 for obviousness, and the rejection of these claims should thus be maintained.

M. Rejection of Claims 1, 2, 5, 6, 8, 9, and 14-60 Based on *Provino* in view of RFC 2504 (Issue No. 17)

Patent Owner presents two responses to this rejection. First, it refers the Office to its response to rejections based on *Solana* in view of RFC 2504. Second Response at 35. This general assertion is not responsive to any of the specific findings of the Office concerning the collective teachings of *Provino* and RFC 2504. Second, Patent Owner asserts that because claims 1 and 36 are not anticipated by *Provino*, they are not obvious over the combined teachings of *Provino* and RFC 2504. *Id.* Finally, Patent Owner states "RFC 920 does not make up for the above-noted deficiencies of *Provino* and RFC 2504" but nowhere identifies what those "deficiencies" relative to the combined teachings of *Provino* and RFC 2504 actually are. *Id.* Patent Owner thus has failed to respond to the specific basis of the obviousness rejection based on *Provino* in view of RFC 2504, and the rejection should be maintained.

N. Rejection of Claims 2-5, 24, 25, 37, 48, and 49 Based on *Provino* in view of RFC 2504 and RFC 920 (Issue No. 18)

Patent Owner contests this rejection by again asserting that claims 1 and 36 are not anticipated by *Provino*, and "RFC 920 does not make up for the above-noted deficiencies of *Provino* and RFC 2504 discussed above." Second Response at 36. Claims 1 and 36 plainly are anticipated by *Provino* (*see* § III.A.), and Patent Owner nowhere identifies any putative

“deficiencies” of the combined teachings of *Provino* and RFC 2504. Because Patent Owner has failed to respond to the specific basis of this rejection, it should be maintained.

O. The Rejection of Claims 10-13 Based on *Provino* in view of RFC 2504, and in further view of *Reed* (Issue No. 19) Was Proper

Patent Owner’s response to this rejection is essentially identical to its response to the rejection of these claims based on *Provino* alone in view of *Reed*. Because that response rests on an incorrect description of what *Reed* actually describes and teaches, and fails to present any response specific to the combined teachings of *Provino* and RFC 2504, considered with *Reed*, this rejection should be maintained.

P. Rejection of Claims 7, 29-32, and 53-56 Based on *Provino* and RFC 2504 in view of *Beser* (Issue No. 20)

Patent Owner does not contest the findings of the Office concerning the collective teachings of *Provino* in view of RFC 2504 and *Beser*. Instead, it simply asserts these claims are not anticipated by *Provino*, RFC 2504 and *Beser* considered individually. Consequently, the Office’s rejection of these claims as being obvious was proper and should be maintained.

V. Rejection of Claims 1-2, 5-6, 8-9, and 14-60 Under 35 U.S.C. § 102(b) and §103 Based on *Beser* (Ground No. 21).

A. Independent Claims 1, 36, and 60

Beser describes DNS systems and processes in which an IP tunnel is securely and transparently established between two network devices with the aid of a third-party trusted network device on a public network. Request at 224-28; First Action at 9-10. Patent Owner has not seriously contested this description of how *Beser*’s DNS systems and processes function. First Response at 24-25. Accordingly, the Office correctly found that *Beser* discloses a DNS system that anticipates independent claims 1, 36 and 60.

As it did in its First Response, Patent Owner bases its response to the rejections based on *Beser* on its belief that the *Beser* systems do not disclose an “indication.” This assumption, in turn, rests on Patent Owner’s assertion that a secure communications link as specified in the claims not only requires use of encryption, but a particular manner of using encryption within that secure communication link. The claims do neither. Thus, like its prior responses, these responses by Patent Owner’ to the rejections based on *Beser* can be ignored.

1. *Beser* Teaches Its DNS Systems Can and Do Use Encryption, and Do Not “Teach Away” from the Claimed DNS Systems

Patent Owner’s theory that *Beser* does not describe a secure communication link rests on its belief that “a secure communication link in view of the specification requires encryption” and *Beser* does not show secure communication links that use encryption. Patent Owner’s assertions are incorrect for at least three reasons.

First, there is nothing in the actual claim language that specifies if or how encryption must be used in the claimed DNS systems. The dependent claims make this unmistakably clear. For example, claim 28, which depends from claim 1, states “the system of claim 1, wherein the secure communication link uses encryption.” Under the well-established doctrine of claim differentiation, claim 1 is necessarily broader in this embodiment than claim 28 – meaning that it can be met by a system that establishes a secure communication link without the use of encryption. Patent Owner is certainly familiar with this doctrine because the Court in *Texas* employed it to reject Patent Owner’s theory that claims require that secure communication use encryption. *Markman* Order, Ex. A to the Comments, at 13. As the Court explained:

VirnetX proposes that a secure communication link is an encrypted link. However, claim 28 of the ’504 Patent covers “[t]he system of claim 1, wherein the secure communication link uses encryption.” ’504 Patent col. 57:17–18. VirnetX’s proposal seeks to import a limitation from dependent claim 28 into independent claim 1, and this violates the doctrine of claim differentiation. See *Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006) (“[C]laim differentiation’ refers to the presumption that an independent claim should not be construed as requiring a limitation added by a dependent claim.”). The specification notes that “[d]ata security is *usually* tackled using some form of data encryption.” ’504 Patent col. 1:55–56 (emphasis added). Therefore, encryption is not the only means of addressing data security. Accordingly, a secure communication link is one that provides data security, which includes encryption. The Court construes “secure communication link” as “a direct communication link that provides data security.”

Markman Order, Ex. A to the Comments, at 13 (italics original, underline emphasis added). In other words, the Court, which employs a more restrictive standard for claim construction than what is used in this proceeding, specifically rejected the precise theory Patent Owner now advances to the Office about this claim element. And even the embodiment specified in claim 28 imposes no restriction on how encryption must or must not be used. Instead, the claim states simply that the “secure communication link uses encryption.”

Patent Owner's resort to the '504 patent specification actually reinforces these conclusions. The specific sentence it quotes plainly does not state that every secure communication link must use encryption – it states “data security is usually tackled using some form of data encryption.” See Second Response at 39 (quoting '504 Patent 1:55-56). Moreover, nothing in this sentence or the claims states that encryption must be used only to encrypt IP packets only after the secure communications link is established. Thus, based on the broadest reasonable construction of the claims, a “secure communication link” does not require use of encryption, and even in the embodiment in claim 28, does not foreclose use of encryption during initiation, but not subsequent to initiation, of the secure communication link. Thus, based on the “broadest reasonable construction” of the claims, *Beser* plainly anticipates the claims, including those requiring “use” of encryption.

As the Request explained, *Beser* shows that during the process of establishing the secure communication link, “the IP 58 packets may require encryption or authentication to ensure the unique identifier cannot be read on the public network 12.”³ Remarkably, Patent Owner contends this showing of use of encryption in establishing the secure communication link “has *nothing to do with the alleged secure communication link* and is thus irrelevant.” Second Response at 39. In short, Patent Owner asks the Office to believe that the interactions between the devices that establish the secure communications link “has nothing to do with the alleged secure communication link.” This theory can be ignored based on its illogical line of reasoning. It must be ignored legally, however, because the claims do not require the particular manner of using encryption asserted by Patent Owner. Patent Owner also ignores that other dependent claims specify uses of encryption other than to encode data being transmitted. For example, claim 5 specifies that encryption is to be used to “authenticate the query using the a cryptographic technique.” *Beser* shows this precise use of encryption where it explains that that IP addresses should be encrypted during the authentication process. Fratto at ¶ 65,67; *Beser* at 11:22-25. Thus, even under Patent Owner's skewed reading of *Beser*, the claims are anticipated. And, of course, because the “encryption” limitation is found only in claim 28, the independent

³ Patent Owner finally concedes that *Beser* does show use of encryption in secure communication links, admitting that *Beser* teaches that queries involving the unique identifier [e.g., a domain name] may be encrypted. Second Response at 39 (citing *Beser* at 11:22-25).

claims are plainly anticipated *Beser*, which even Patent Owner cannot dispute discloses establishment of secure IP communication links.

Second, the Office already rejected Patent Owner's contentions that *Beser* teaches away from using encryption. ACP at 32. A plain reading of the *Beser* specification shows that it does not state that using encryption in IP tunneling schemes is "undesirable" regardless of the nature of the volume of data being sent through the IP tunnel. Instead, as the Office correctly observed, *Beser* teaches a method of securing the readable source address of an IP packet, which is a field that encryption does not protect. ACP at 32. The Office also observed that, within the *Beser* scheme, "[o]f course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ('IPSec')." ACP at 32 (quoting *Beser* at 1:54-56). As the Requester pointed out, this passage in *Beser* makes unmistakably clear that the IP traffic is ordinarily encrypted IP tunnels established using the IPSec protocol. Request at 224-25; Comments at 19-21. Patent Owner also mischaracterizes passages in *Beser* that explain that a decision to not use encryption will be driven by practical considerations, such as the volume of data being transmitted for certain data types (i.e., VOIP and multimedia), the capacity of a particular hardware setup to handle that volume and cost considerations. Fratto at ¶¶64-65. Importantly, in these passages, *Beser* explains that these practical concerns do not always arise for the two high volume data types being discussed, and do not arise at all for other data transfer situations. *Id.*; *Beser* at 1:54-66. Consequently, even a lay person would recognize from *Beser* that encryption is ordinarily used in IP tunneling applications – because that is what IPSec specifies should be done – and that the decision to not use encryption would arise only in unique situations (i.e., situations involving high volume data transfers where costs considerations limit computational power available).

Patent Owner also again ignores the actual claim language. As noted above, claims 1, 36 and 60 do not require use of any encryption in their broadest reasonable construction. Patent Owner's extensive debate about whether *Beser* "teaches away" from systems that use encryption is thus legally irrelevant to these claims. Moreover, even for claims that may require some "use of encryption," those claims plainly are not restricted to the high volume data transfer situations that were the subject of *Beser*'s cautions. Patent Owner simply ignores this point, which was clearly conveyed in the Request, the First Action, the Comments and the ACP. Request at 224-25; First Action at 10; Comments at 19-21; ACP at 32. Indeed, Patent Owner's entire "teaching

away” theory rests on series of fundamental errors about the claims in the ’504 patent (i.e., that they uniformly require a particular manner of using encryption, and that they are limited to situations involving the examples of high data volume transfers discussed in *Beser*).

Consequently, *Beser*’s cautions about using encryption within IP tunnels established pursuant to the IPsec protocol in high data volume applications are legally irrelevant to the ’504 claims.

2. *Beser* Teaches a DNS System that Comprises an “Indication” Specified in Claims 1, 36, and 60

The Office correctly explained that *Beser* discloses a DNS system that is configured to “comprise an indication that the domain name service system supports establishing a secure communication link” (and corresponding provisions in claims 36 and 60). First Action at 9-10; ACP at 33-34. In response, Patent Owner presents two alternative theories why it believes this finding was incorrect. First, Patent Owner states that “if the Office construes the recited indication to be a ‘visible message or signal to a user...’ then this is not taught by *Beser*. This hypothetical reading of the claims by the Office can be ignored – the Office plainly did not construe the “indication” to be limited to one specific type of indication. Instead, the Office explained that the term “indication” as used in the claims and as discussed in the specification has a broad meaning. For example, in the ACP, the Office observed that the term “indication” had “no special meaning in view of specification” because the ’504 “specification does not use this term specifically.” ACP at 33. Thus, the Office observed that construing “the claimed ‘indication’ as a provision of an address” is appropriate given that the term “is reasonably broad consistent with the specification.” ACP at 34. The Office also observed that the Court in the co-pending litigation reached the same conclusion. *Id.* The Office’s concluded that, in light of the absence of an explicit and narrow definition compelled by the claim language or the specification, an “indication” could be construed to include a “visible message or signal to a user.” ACP at 33. The Office is correct – the language used in the claims does not impose any requirements as to the form or manner by which the required indication must be provided, and nothing in the claims or the specification limits “indication” to a visible message to a user.

Second, the Office’s comments demonstrate that Patent Owner’ alternative theory – that the claims foreclose reading an indication to be “merely returning an IP address” – is also flawed and can be ignored. On this point, not only does Patent Owner ignore the fact that the claims impose no such restriction, it seriously mischaracterizes what *Beser* actually shows. For

example, *Beser* explains that in its example of a VOIP implementation, a unique identifier may be a user's email address or phone number, and this associates the user with the mechanism used to establish the secure IP tunnel carrying the VOIP traffic. *See Beser* at 10:52-66. In these examples, the unique identifier can provide an indication "visible to a user" because the identifier is information that can be understood and used by a person. Moreover, when the components in the *Beser* systems are interacting with each other to establish a secure IP communication link, they necessarily act on "indications" associated with the destination as well as the data being transferred (e.g., dictating whether to attempt to establish a tunnel or not).

Because each of Patent Owner's two theories would require the Office to read limitations from the specification into the claims, they should be rejected. The Office's correctly found claims 1, 36 and 60 anticipated by the *Beser* DNS systems under 35 U.S.C. § 102(e).

B. Dependent Claims 16, 17, 27, 33, 40, 41, 51 and 57 (Issue No. 21)

The Office correctly found that *Beser* discloses the limitations of dependent claims 16, 17, 27, 33, 40, 41, 51, and 57. ACP at 10. Patent Owner presents no response specific to any of these claims, but simply refers to its response to the rejection of claims 1 and 36 over *Beser*. Patent Owner thus concedes that these claims are not patentably distinct from claims 1 and 36. Because the rejection of claims 1 and 36 over *Beser* was proper, the rejection of claims 16, 17, 27, 33, 40, 41, 51 and 57 was also proper.

C. Dependent Claims 18 and 42 (Issue No. 21)

The Office correctly found that *Beser* discloses every limitation of claims 18 and 42, including that "at least one of the plurality of domain names is reserved for secure communication links." In response, Patent Owner asserts "the Office eviscerates the meaning of the claim language by asserting that the domain names that are allegedly 'reserved' for secure communications links need not be used for secure communication links." Second Response at 14. Patent Owner is incorrect, and misrepresents the Office's findings. The Office explained that *Beser* teaches that in certain circumstances "domain names are reserved for secure communication links." ACP at 35. The Office also explained that nothing in the claims requires that "the initiator . . . take advantage of the reservation." ACP at 23-24. Once again, Patent Owner's response represents an attempt to import an unclaimed limitation into claims 18 and 42 (e.g., that the "reserved" domain names must actually be used only for secure communication

links). For reasons already stated by the Office, this is improper. ACP at 35. Consequently, the rejection of claims 18 and 42 as anticipated by *Beser* was proper.

D. Dependent Claims 24 and 48 (Issue Nos. 21 and 22)

The Office correctly found that *Beser* discloses every element of dependent claims 24 and 48, including that “at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link.” For example, in the First Action, the Office correctly determined that *Beser* teaches the functional correlation between a secure domain name (e.g., that it is associated with a certificate) and establishing a secure communication to that domain. First Action at 10. Patent Owner disagrees and simply incorporates by reference its arguments made in response to rejections based on *Solana*. For the reasons provided above in section II.A.6., the Office correctly found that a domain name per se is nonfunctional descriptive material incapable of differentiating the claims from the prior art.

Patent Owner’s assertion that the Office and the Requester “never substantively addresses the claimed features or Patent Owner’s arguments” concerning *Beser* is simply false. The Request, and the First Action, each explained in detail why indications within the *Beser* scheme comprise “an indication the domain name service system supports establishing a secure communication link.” Request at 231-32; First Action at 9-10. For example, the Office and Requester explained that the *Beser* system shows DNS systems that use particular secure names (including secure domain names) that are required to authenticate and establish a secure communications linked to that secure domain. Request at 238-39; ACP at 36. The fact that the Office’s made observations in the ACP responding to unpersuasive and irrelevant comments from Patent Owner does not change its previous findings. Consequently, the Office’s rejections of 24 and 48 claims as anticipated by *Beser* was proper and correct, and should be maintained.

E. Dependent Claims 26 and 50 (Issue No. 21)

The Office correctly found that *Beser* discloses “at least one of the plurality of domain names enables establishment of a secure communication link.” ACP at 36. Patent Owner responds by again asserting that the *Beser* DNS systems “merely [return] an address based on a domain name query...” Second Response at 43. Patent Owner again mischaracterizes how the *Beser* DNS systems function, and ignores the fact that the claims are not restricted to the narrow

meaning it contends they should have. Consequently, Patent Owner's response to the rejection of claims 26 and 50 should be ignored, and the rejection of these claims should be maintained.

F. Dependent Claims 2, 5-7, 14, 15, 19-23, 25, 28-32, 34, 35, 37-39, 43-47, 49, 52-56, 58, and 59 (Issue No. 21)

The Office correctly found that *Beser* anticipates claims 2, 5-7, 14, 15, 19-23, 25, 28-32, 34, 35, 37-39, 43-47, 49, 52-56, 58, and 59. ACP at 10. In response, Patent Owner refers simply to its response to the rejection of claims 1 or 36 over *Beser*. Because those claims were properly rejected and no distinct reasons offered by Patent Owner, the rejection should be maintained.

G. Dependent Claims 2-5, 24, 25, 37, 48, and 49 (Issue No. 22)

Patent Owner presents no response to any of the specific findings of the Office that *Beser* in view of RFC 920 renders claims 2-5, 24, 25, 37, 48, and 49 obvious. Instead, it simply contends that *Beser* considered alone does not anticipate claim 1. Second Response at 44. Consequently, the Office's rejection of these claims was proper and should be maintained.

H. Dependent Claims 8 and 9 (Issue No. 23)

Patent Owner presents no response to any of the specific findings of the Office that *Beser* in view of RFC 2401 renders claims 2-5, 24, 25, 37, 48, and 49 obvious. Instead, it simply contends that *Beser* considered alone does not anticipate claim 1. *Id.* Consequently, the rejection of claims 8 and 9 was proper and should be maintained.

I. Dependent Claims 10-13 (Issue No. 24)

The Office rejected claims 10-13 in the First Action as being obvious based on *Beser* in view of RFC 2401, in further view of *Reed*. First Action at 10; First Response at 5-8. The only basis Patent Owner presented in its First Response to these rejections was that *Reed* was not proven to be prior art. The Office did not find this argument persuasive. Now, in its Second Response, Patent Owner contests for the first time the findings adopted in the First Action regarding *Reed*. Patent Owner's belated response to the First Action should be disregarded as it is inconsistent with 37 C.F.R. 1.951. Patent Owner also presents no response specific to the combination of *Beser*, RFC 2401 and *Reed*, but simply refers to other portions of its Second Response to contend that *Reed* does not disclose certain elements of claims 10 and 12. Second Response at 44-45. Because that reading of *Reed* is incorrect (*see* § II.C. above), its response to the rejections of claims 10 and 12 here is also unpersuasive. Moreover, Patent Owner presents

no response regarding claims 11 and 13. Consequently, the Office's rejection of claims 10-13 as being obvious based on *Beser* in view of RFC 2401, in further view of *Reed* was proper.

VI. Response to Patent Owner's Arguments Regarding Rejection of Claims 1-2, 5-6, 8-9, and 14-60 Based on RFC 2230 (Issue No. 25)

A. Independent Claims 1, 36, and 60

As explained in the Request and confirmed by the Office, RFC 2230 describes a system that uses a security extension (the KX record) in DNS systems to enable support of secure communications over the Internet. Request at 276-79; ACP at 37-38. RFC 2230 describes the details of the KX record structure, and identifies requirements and designs for using it in DNS systems, including systems compliant with IPsec and other authorization and encryption techniques. Request at 279-78; Comments at 26. Consequently, the Office properly found that RFC 2230 describes "DNS systems" that anticipate independent claims 1, 36 and 60.

In its Second Response, Patent Owner now asserts that (i) Routers R1 and R2 are not DNS system components and (ii) RFC 2230 does not teach DNS systems that "comprise an indication." Neither assertion is correct.

1. RFC 2230's Routers "R1" and "R2" Are Plainly A Functional Component of the RFC 2230 DNS Systems

The First Action and the Request explained that RFC 2230 discloses not only a DNS server but other components, particularly routers "R1" and "R2," that are delegated functionality of the secure DNS system. First Action at 10-11; Request at 276-81. These distributed components in RFC 2230 operate in a coordinated manner to evaluate requests to establish secure communications, such as authentication of domain names and other functions that are essential to the establishment of a secure communication link. First Action at 10-11; Request at 276-81. In its First Response, Patent Owner asserted routers R1 and R2 are not part of the DNS systems shown in RFC 2230. The Office disagreed, pointing out, *inter alia*, that the R1 and R2 notes are delegated functions and are authorized to act on behalf of the DNS system as a key exchanger. ACP at 37-38. ("RFC [2230] explicitly teaches that key exchange nodes (edge router R1 and R2 are intertwined with the DNS system.").

Patent Owner again presses its flawed theories about the roles of R1 and R2 in the DNS systems described in RFC 2230. Second Response at 45-46. Although Patent Owner now concedes that R1 and R2 do interact in a domain name service exchange with the domain name

server, it contends that for some reason this is insufficient to impart on R1 and R2 a status equivalent to various components described in the '504 patent disclosure as making up a “DNS system.” In particular, Patent Owner asserts contends R1 and R2 do not possess some unspecified set of “DNS functions” that components shown in the '504 disclosure do. *Id.* at 45.

Patent Owner’s theory also, again, ignores what the claims actually specify and what RFC 2230 actually describes. Critically, the '504 claims do not expressly or implicitly specify a particular nature of functionality that components within a DNS system must or must not possess. Patent Owner’s theories again seek to improperly import limitations from its specification into the claims. The difference in this instance is that Patent Owner cannot even articulate what these limitations are – instead, it calls them simply “DNS functions.”

The distinctions Patent Owner attempts to make between the RFC 2230 DNS systems and the claimed DNS systems are thus simply illusory. First, Patent Owner asserts that the relationship between R1/R2 and the DNS servers they interact with is “threadbare” and limited to the running of a DNS lookup. This is plainly incorrect based on what RFC 2230 itself explains. For example, RFC2230 explains that in the first subnet-to-subnet 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. ...

In this example and others, RFC 2230 explains that R1 and R2 are key exchange nodes to which the KX records direct requests for determining whether to, and how to route IP traffic. R1 and R2 thus play a role integral to the secure DNS systems being described in RFC 2230. *See* ACP at 38. Indeed, the only way Patent Owner could conclude otherwise is to simply ignore what RFC 2230 actually states.

Patent Owner next asserts that the role of the key exchange nodes (routers R1 and R2) in the DNS systems of RFC 2230 is simply to “act on behalf of nodes S and D – not on behalf of the DNS system, which is not described to be a node.” Specifically, Patent Owner contends that RFC 2230 does not teach “that the DNS delegates a proxy router (e.g., R2) to perform key-related authorization on its behalf” because “the plain teachings of RFC 2230 describe proxy routers R1 and R2 as delegated to act on behalf of nodes S and D—not on the DNS system.” Second Response at 47 (emphasis added). Once again, Patent Owner is simply wrong. RFC 2230 makes absolutely clear that R1 and R2 are delegated functions of the DNS system. As the Office explained in the ACP, RFC 2230 teaches that “the ‘KX record is useful in providing an

authenticable method of delegating authorization for one node to provide key exchange services . . . on behalf of the delegator (DNS) rather than becoming an independent entity. ACP at 37 (citing RFC 2230 at §1). Indeed, the text following the very example cited by Patent Owner in RFC 2230 at § 2.1.1 refutes Patent Owner’s theory. As that section explains, “[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.” (emphasis added). In other words, contrary to Patent Owner’s assertions, R1 is not acting “on behalf of S and D,” it is acting independently of these two nodes to determine whether to and how to route IP traffic between these nodes – the exact function of the claimed DNS systems. The Office thus correctly rejected Patent Owner’s contention, noting that the “delegate (the key exchange node) . . . acts on behalf of the delegator (DNS) rather than becoming an independent entity.” ACP at 37 (emphasis in original). Patent Owner’s description of Fig. 2 is similarly flawed, and can be simply ignored as it is superfluous. Of course, none of these putative distinctions correspond in any manner to actual claim limitations, and the ’504 specification does not contain an explicit definition of a “DNS system” that would exclude the DNS systems described in RFC 2230. Consequently, Patent Owner’s flawed theories about what RFC 2230 teaches can simply be ignored.

Patent Owner’s next attack on RFC 2230 is its flawed assertion that it does not “properly incorporate” RFC 2065. Here, Patent Owner is incorrect on the law and the facts. The schemes described in RFC 2230 build upon and use the systems and practices described in RFC 2065, which RFC 2230 explains at § 1 describes “standards-track security extensions to the DNS” upon which the KX scheme described in RFC 2230 functions. The references in RFC 2230 to RFC 2065 are describing what the KX schemes shown in RFC 2230 comprise and how they function. For example, RFC 2230 states that “KX records MUST always be signed using method(s) defined by the DNS Security extensions specified in [RFC 2065].” RFC 2230 at 9; *see also* RFC 2230 at 1. Thus, even if Patent Owner’s “incorporation by reference” theory was relevant, RFC 2230 satisfies this standard as it uses “broad and unequivocal” language referring to the other prior art document. *See Harari*, 656 F.3d at 1335.

2. RFC 2230 Discloses “a Domain Name Service System Configured to . . . Comprise an Indication...”

In the ACP, the Office correctly found that RFC 2230 discloses “a Domain Name Service System configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link.” ACP at 37-38. In its Second Response, Patent Owner agrees that the term “indication” may be a “visible message or signal to a user that the DNS system supports establishing a secure communication link” but argues that the Office did not use this construction of “indication.” Response at 48.

Patent Owner misrepresents the Office’s findings. As discussed elsewhere in these comments, the Office confirmed that the claim term “indication” should be construed broadly to include “a visible message or signal to a user,” which, for instance, would include the “establishment of a VPN.” ACP at 18. Because RFC 2230 shows DNS systems that permit a VPN to be established, thereby permitting communications between domains discernible to the user, it discloses a DNS system comprising the claimed “indication.” Patent Owner again tries to import unclaimed limitations into the claims, asserting that RFC 2230 describes a DNS system that “is nothing more than a conventional DNS system similar to those disparaged and disclaimed in the ’504 patent specification.” Response at 48-49. Patent Owner grossly mischaracterizes RFC 2230, ignoring that, beyond the functionality that it believes is conventional, RFC 2230 teaches delegating key exchange authorization in DNS systems. ACP at 38. More directly, the claims do nothing to exclude from their scope some unspecified “conventional” DNS system – “derogatory” comments in the patent specification are not claim limitations. Accordingly, the Office correctly found that the DNS systems in RFC 2230 – “conventional” or not – comprise “an indication that the Domain Name Service System supports establishing a secure communication link.” The Office’s rejection of these claims as being anticipated by RFC 2230 was therefore proper.

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

The Office correctly found RFC 2230 anticipates claims 16, 17, 27, 33, 40, 41, 51, and 57. Patent Owner presents no response specific to any of these claims, but simply refers to its response to the rejection of claims 1 and 36 over RFC 2230. Patent Owner thus concedes these claims are not patentably distinct from claims 1 and 36, and that the rejections were proper.

C. Dependent Claims 18 and 42

The Office correctly found that RFC 2230 discloses “at least one of the plurality of domain names is reserved for secure communication links.” In response, Patent Owner repeats its theory that “the Office eviscerates the meaning of the claim language by asserting that the domain names that are allegedly ‘reserved’ for secure communications links need not be used for secure communication links.” Second Response at 50. Patent Owner is incorrect, and misrepresents the Office’s findings. The Office explained that, in certain circumstances explained in RFC 2230 related to KX records, “domain names are reserved for secure communication links,” which is all that the claims require. ACP at 39. As the Office explains, nothing in the claim requires that “the initiator . . . take advantage of the reservation.” ACP at 39. Consequently, the Office’s rejection of claims 18 and 42 were proper.

D. Dependent Claims 24 and 48

The Request provided a detailed explanation how RFC 2230 anticipated claims 24 and 48 (i.e., it discloses DNS systems that comprise an indication the DNS system supports establishing a secure communication link). The Office adopted these findings, and rejected claims 24 and 48 as anticipated. Despite this clear record, Patent Owner somehow concludes the Office “determined that RFC 2230 does not disclose the additional features recited in claims 24 and 48.” Second Response at 50. This is plainly wrong. In fact, the Office observed in the ACP that RFC 2230 teaches a functional correlation between a secure domain name (e.g., one associated with a KX Record) and establishing a secure communication to that domain. ACP at 39-40. The Office also refuted Patent Owner’s theory that the claims require the domain name itself to be an “indication,” explaining that such a theory sought to impermissibly distinguish the claims from RFC 2230 using non-functional descriptive material. Again, Patent Owner changes its stance, and now asserts the claims “describe a functional relationship” between domain names and secure DNS systems. Yet, this is precisely what is taught by RFC 2230 – a functional relationship between domain names associated with KX records and the use of these records by DNS systems to authenticate and establish a secure communications link to that secure domain. The Office thus correctly found that RFC 2230 describes DNS systems comprising “indications” that the RFC 2230 DNS systems support secure communication links (ACP at 39-40), and the rejection of claims 24 and 48 as anticipated by RFC 2230 was proper.

E. Dependent Claims 26 and 50

The ACP confirmed the findings in the First Action and the Request that RFC 2230 discloses DNS systems that comprise at least one domain name that “enables establishment of a secure communication link.” ACP at 40. The reason for this conclusion is simple – RFC 2230 explains that KX records are associated with a secure domain name and are used to authenticate and establish secure IP tunnels to the domain associated with the KX record. *See, e.g.*, RFC 2230 at § 2. Thus, RFC 2230 discloses a DNS system that uses KX records to enable establishment of secure communication links, and anticipates claims 26 and 50.

In response, Patent Owner invents yet another new unclaimed theory about the claims; namely, that they exclude an “attenuated relationship” between a user and a secure communication link. Patent Owner’s theory is not only irrelevant, as there are no claim limitations that permit or exclude some unspecified degree of “attenuation” between a “user” and the secure communication link, it is effectively unintelligible. For example, Patent Owner asserts that it has “disparaged and disclaimed” these unspecified “attenuated” connections and points to random observations in the ’504 specification discussing *optional* ways of implementing user interface controls for using DNS systems (e.g., that a user can “enable a secure communication link using a single click of a mouse.”) Second Response at 51. Nothing in the claim language can even remotely be ascribed to its obscure theory. Patent Owner also makes an illogical claim that because it is the “KX records themselves, not any domain name, [which] enables establishment of secure communication link,” this somehow demonstrates the claims are not anticipated. Yet, RFC 2230 explains that KX records are associated with specific, secure domains and are used to establish links to those domains, precisely as the claims specify. See RFC 2230 at § 2, 2.1. Indeed, RFC 2230 teaches that the initiator must query the DNS system with a domain name query, where the response indicates via KX records that 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. ACP at 40. Thus, RFC 2230 teaches that a domain name can enable establishment of a secure communications link, and anticipates claims 26 and 50.

F. Dependent Claims 2, 6, 14, 15, 19-23, 25, 27, 28-32, 34, 35, 37-39, 43-47, 49, 50, 52-56, 58, and 59

The Office correctly found that RFC 2230 anticipates dependent claims 2, 6, 14-17, 19-22, 25, 27-35, 37-41, 43-46, 49, and 51-59. ACP at 11. Patent Owner responds by simply asserting that claims 1 and 36 are not anticipated. Patent Owner thus concedes that these claims

are not patentably distinct from claims 1 and 36. Because claims 1 and 36 are anticipated by RFC 2230, the recited claims are also anticipated, and the rejections should be maintained.

G. Rejection of Dependent Claims 2-5, 24, 25, 37, 48, and 49 Based on RFC 2230 in View of RFC 920 (Issue No. 26)

1. Dependent Claim 5

In its First Response, the sole basis raised by Patent Owner in response to the rejection of claim 5 based on RFC 2230 in view of RFC 920 was that claim 1, from which claim 5 depends, was not anticipated by RFC 2230. First Response at 35. Now, in its Second Response, Patent Owner for the first time disputes the findings adopted in the First Action regarding claim 5, contrary to 37 C.F.R. 1.951. The Office should disregard these new assertions. The substance of these assertions also is incorrect. RFC 2230 describes examples of secure connections established using IPsec. See RFC 2230 at § 2.1. Under IPsec, cryptographic techniques, such as digital certificates (e.g., KX records), may be used to authenticate users. See RFC 1825 at § 3.1. Perhaps recognizing this, Patent Owner again raises its “improper incorporation by reference” theory, asserting that RFC 2230 has not properly incorporated by document describing the IPsec standard (i.e., RFC 1825.) Yet, RFC 2230 plainly identifies RFC 1825 (see RFC 2230 at pages 1-2), which describes the IPsec standard used to implement the examples shown in § 2.1. Thus, RFC 2230, in view of RFC 920, plainly shows a DNS system configured to “authenticate the query using a cryptographic technique” as specified in claim 5.

2. Dependent Claims 24 and 48

The Office correctly found claims 24 and 48 obvious based on RFC 2230 in view of RFC 920. Specifically, RFC 2230 describes use of KX records associated with secure domain names to establish secure connection links to secure domains associated with those KX records. Claims 24 and 48 are thus anticipated by RFC 2230. In addition, to the extent Patent Owner were to contend the choice of a domain name were somehow implicated by claims 24 and 48, such a choice would have been obvious, given the guidance in RFC 920, *inter alia*, that new top-level names may be developed, that those names are usually human-understandable terms, and may be freely selected. Request at 310-311. See also Request at 286-87, 298-99. In response, Patent Owner contends RFC 920 does not support the rejection, asserting that reliance on RFC 920 is “fatally infected with hindsight bias,” and, remarkably accuses the Office of failing to provide “articulated reasoning” for the rejection. Second Response at 53-54. The reasoning supporting

the conclusion of obviousness is plainly set forth in the Request, which was incorporated by reference in the ACP. ACP at 12. Consequently, the Office's rejection of claims 24 and 48 as obvious based on RFC 2230 in view of RFC 920 was proper. Finally, Patent Owner presents no response to the rejection of dependent claims 2-4, 25, 37 and 49 other than that the claims from which these claims depend are not anticipated by RFC 2230. Consequently, the Office's rejection of these claims as obvious based on RFC 2230 in view of RFC 920 was proper.

H. Rejection of Dependent Claims 8 and 9 Based on RFC 2230 in View of RFC 2401 (Issue No. 27)

Patent Owner does not specifically contest any of the findings of the Office in the ACP based on RFC 2230 in view of RFC 2401, but instead relies on its positions stated with respect to RFC 2230 alone. Consequently, the rejection of claims 8 and 9 as set forth in the ACP as being obvious based RFC 2230 in view of RFC 2401 was proper.

I. Rejection of Claims 10-13 based on RFC 2230 in View of RFC 2401 and in Further View of *Reed* (Issue No. 28)

The Office rejected claims 10-13 in the First Action as being obvious from RFC 2230 in view of RFC 2401, in further view of *Reed*. First Action at 11. In response, Patent Owner asserted only that *Reed* was not prior art. First Response at 5-8. Now, in its Second Response, Patent Owner contests for the first time the Office's substantive findings regarding *Reed* in the First Action. Again, Patent Owner's belated response is inconsistent with 37 C.F.R. 1.951 and should be disregarded. In addition, Patent Owner presents no response specific to the combination of RFC 2230, RFC 2401 and *Reed*, but simply points to its comments regarding combinations of other prior art with *Reed*. Because those comments rest on mischaracterizations of *Reed*, they should be ignored. In addition, no response was provided by Patent Owner to the rejection of claims 11 and 13. Consequently, the rejection of claims 10-13 as being obvious over RFC 2230, 2401 and *Reed* was proper.

J. Rejection of Claims 29-32 and 53-56 Based on RFC 2230 in view of *Beser* (Issue No. 29)

Patent Owner asserts simply that dependent claims 29-32 and 53-56 depend from claims 36 and contends incorrectly that RFC does not disclose "an indication that the domain name service system supports establishing a secure communication link." No response was provided

to the specific combination of RFC 2230 and *Beser*. Consequently, the Office's rejection of these claims as obvious based on RFC 2230 in view of *Beser* was proper.

VII. Rejection of Claims 1, 2, 6, 14-22, 24-46, 48-52, and 57-60 Under 35 U.S.C. § 102(b) based on RFC 2538 (Issue No. 30)

A. Independent Claims 1, 36, and 60

The Office found that RFC 2538 anticipates independent claims 1, 36, and 60. Request at 322-25, 333-36, 347-49; First Action at 12. In response, Patent Owner contends that RFC 2438 does not disclose (i) any means of retrieving a CERT RR, (ii) any entity that may obtain a CERT RR and (iii) does not disclose any queries to a DNS. Second Response at 56. Patent Owner's assertions derive from its failure to use the statutorily required perspective of a person of ordinary skill in the art. Indeed, Patent Owner seems to be taking the position that anything not explicitly written into the text of RFC 2538 would be unknown and unknowable to a person of ordinary skill. Patent Owner is plainly wrong. RFC 2538 describes a scheme that is designed to function within DNS systems, which means that DNS systems are necessarily taught by RFC 2538. For instance, RFC 2538 is unambiguous that it "specifies an Internet standards track protocol for the Internet community" and that it is intended to be used within a "Domain Name System." RFC 2538 at Status of the Memo; Abstract. One of ordinary skill also would have recognized that such a system includes an initiator establishing a connection with a target using a DNS server. First Action at 12-13. While Patent Owner claims the components of DNS systems are not inherently disclosed by RFC 2538, it presents no reasons why this is the case, simply repeating they are not explicitly written down in RFC 2538. The Office's conclusions that the claims are anticipated are thus correct. ACP at 41-42.

Patent Owner also again claims that the Office has failed to employ its construction of "indication" as being "a visible message or signal to a user," which, for instance, would include the "establishment of a VPN." ACP at 18. Again, Patent Owner misunderstands the Office's construction of "indication" as discussed above. Patent Owner also repeats its legally unsupported theory that subject matter "disparaged" as being known in the prior art may be implicitly, rather than explicitly, excluded from the claims. Second Response at 57-58. This is simply incorrect under the broadest reasonable construction standard used by the Office. Accordingly, the Office correctly found that RFC 2538 anticipates claims 1, 36 and 60.

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

The Office correctly found that RFC 2538 anticipates dependent claims 16, 17, 27, 33, 40, 41, 51, and 57. Patent Owner presents no response specific to any of these claims, but simply refers to its response to the rejection of claims 1 and 36 over RFC 2538. As such, Patent Owner concedes that these claims are not patentably distinct from claims 1 and 36, and because the rejection of claims 1 and 36 was proper, the rejection of these claims also is proper.

C. Dependent Claims 18 and 42

The Office correctly found that RFC 2538 discloses that “at least one of the plurality of domain names is reserved for secure communication links.” In response, Patent Owner again claims “the Office eviscerates the meaning of the claim language by asserting that the domain names that are allegedly ‘reserved’ for secure communications links need not be used for secure communication links.” Second Response at 59. As explained above, Patent Owner is incorrect, and misrepresents the Office’s findings. The Office explained that, in certain circumstances explained in RFC 2538 related to a CERT RR, a “domain names are reserved for secure communication links,” which is all that the claims require. ACP at 39. As the Office explains, nothing in the claim requires that “the initiator . . . take advantage of the reservation.” ACP at 43. Thus, as it does elsewhere, Patent Owner seeks to distinguish RFC 2538 on the basis of unclaimed limitations. The Office considered and correctly rejected Patent Owners theory. ACP at 43. Consequently, the rejection of claims 18 and 42 as anticipated by RFC 2538 was proper.

D. Dependent Claims 26 and 50

The Office correctly found that RFC 2538 anticipates dependent claim 26 and 50. In response, Patent Owner repeats its flawed “attenuation” theory; namely, that because the ’504 disclosure “disparaged” certain ways a domain name “enables establishment of a secure communication link,” these various ways must be excluded from the literal scope of the claims. Second Response at 59. Patent Owner again is wrong, Patent Owner also contends its systems do not require more than “minimal inputs” – but again, these are unclaimed limitations (if they even exist as contended). Second Response at 59-60. The Office correctly rejected these arguments. ACP at 44-45. Indeed, 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 domain name and/or IP address. ACP at 45; Comments, pp 79 & 80; Fratto Dec. at 79 & 80. Thus, the domain name enables

establishment of a secure communications link, and the Office's rejection of these claims as being anticipated by RFC 2538 was proper.

E. Rejection of Claims 3, 4, 24, 25, 48, and 49 Based on RFC 2538 in View of RFC 920 (Issue No. 31)

Patent Owner presents no response to the rejection of claims 3, 4, 24, 25, 48, and 49 distinct from its response to the rejection of claims 1 and 36. Because the rejection of claims 1 and 36 was proper, the Office's rejection of claims 3, 4, 24, 25, 48, and 49 claims as obvious based on RFC 2538 in view of RFC 2401 was proper.

F. Rejection of Claims 8 and 9 Based on RFC 2538 in View of RFC 2401 (Issue No. 32)

Patent Owner presents no response to the rejection of claims 8 and 9 distinct from its response to claims 1 and 36. Because the rejection of claims 1 and 36 was proper, the Office's rejection of claims 8 and 9 as obvious based on RFC 2538 in view of RFC 2401 was proper.

G. Rejection of Claims 10-13 Based on RFC 2538 in view of RFC 2401 in Further View of *Reed* (Issue No. 33)

The Office rejected claims 10-13 based on RFC 2538 in view of RFC 2401, and further in view of *Reed*. First Action at 12; First Response at 5-8. In response, Patent Owner contended simply (and incorrectly) that *Reed* was not prior art. Now, in its Second Response, Patent Owner for the first time contests the findings in the First Action regarding *Reed*, contrary to 37 C.F.R. 1.951. Patent Owner's substantive description of *Reed* is also incorrect, as explained above. See § II.C. Consequently, the rejection of claims 10-13 was proper.

H. Rejection of Claims 29-32 and 53-56 Based on RFC 2538 in View of *Beser* (Issue 34)

Patent Owner presents no response to the rejection of claims 29-32 and 53-56 that is distinct from its response to claims 1 and 36. Because the rejection of claims 1 and 36 was proper, the Office's rejection of claims 29-32 and 53-56 as obvious based on RFC 2538 in view of *Beser* also was proper.

I. Rejection of Claims 5, 23, and 47 based on RFC 2538 in View of RFC 2065 (Issue 35)

Patent Owner presents no response to the rejection of claims 5, 23, and 47 that is distinct from its response to claims 1 and 36. Because the rejection of claims 1 and 36 was proper, the

Office's rejection of claims 5, 23, and 47 claims as obvious based on RFC 2538 in view of RFC 2065 also was proper.

VIII. There are No Secondary Considerations Linked to the Claims

The Office correctly found no nexus between the putative evidence of secondary considerations presented by Patent Owner and the claimed inventions. ACP 46-48. Its conclusions were correct, given that Patent Owner presented no evidence that any specifically claimed features of the claimed DNS systems could be identified as being attributable to any commercial success of any product or service. The Office also was correct to not give any weight to the highly biased, self-interested and unsupported testimony of Patent Owner's Chief Technology Officer, Robert Short. Nothing identified by Patent Owner or its self-interested witness establishes with a legitimate evidentiary basis that any putative secondary considerations exist that can be attributed to any of the claimed inventions as distinguished from features of products and services known in the prior art, given that claims 1-60 encompass prior art DNS systems. Finally, evidence of licensing or a jury verdict that is not the subject of a final judgment in concurrent litigation simply is irrelevant – neither constitutes “evidence of commercial success” much less evidence of secondary considerations relevant to the claims. MPEP § 716.03.

For all of the reasons set forth above, Patent Owner has not rebutted the Office's rejections of the claims on any of Issues 1-35, and that nothing raised in Patent Owner's Second Response merits reopening prosecution of the '504 patent. The rejection of all the claims under each of those Issues should, accordingly, be maintained.

Respectfully submitted,

/ Jeffrey P. Kushan /
Reg. No. 43,401
Attorney for Third Party Requester

SIDLEY AUSTIN LLP
1501 K Street, N.W
Washington, D.C. 20005

tel. (202) 736-8000/ fax (202) 736-8711

Date: January 23, 2013