IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of U.S. Patent No. 6,502,135 Edmund Colby Munger et al. Issued: December 31, 2002 For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	Control No.: 95/001,682 Group Art Unit: 3992 Examiner: Behzad Peikari Confirmation No.: 1074

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:

On May 14, 20102, Patent Owner filed an overlength response ("Response") to the February 15, 2012 Office action ("Office Action") and a petition under 37 C.F.R. § 1.183 seeking waiver of the page limit for that response. On September 18, 2012, the Office granted Patent Owner's petition. This response is timely filed within the 30-day period set by the decision on the petition. Third Party Requester believes that no fee is due in connection with the present response. However, any fee determined to be required for entry or consideration of this paper may be debited from Deposit Account No. 18-1260.

- A table of contents is provided at pages ii to iv. Requester submits the table of contents is not counted against the page limits applicable to this response. Should the Office determine otherwise, the Office is requested to disregard the table of contents.
- The response to the Patent Owner Comments begins on page 1.

Table of Contents

I. Introduction

Requestor urges the Examiner to maintain the rejections of claims 1-18 set forth in the Office Action dated 15 February 2012 (the "Office Action").

II. Response to Patent Owner Contentions on Status of References as Prior Art.

On pages 5-18 of the Response, Patent Owner asserts there is "no evidence" that the *Aventail, BinGO!, Kent*, *Reed*, *Wang* and "RFCs" are prior art under 35 U.S.C. § 102(a) or (b). Patent Owner's claims border on the frivolous – each reference is unquestionably a printed publication, and only by studied ignorance of the facts can Patent Owner assert otherwise.

Initially, Patent Owner grossly misstates Requestor's burden to provide evidence establishing that the documents are printed publications. According to Patent Owner, Requestor was required to provide "a showing" with "evidence proving" the date each reference was made publically available. Response at 6. This is incorrect – all that is required is that Requester represent that the reference was, in fact, published. Indeed, the submission of a paper by a party is a certification that "[t]o the best of the party's knowledge, information and belief, formed after an inquiry reasonable under the circumstances… [t]he allegations and other factual contentions have evidentiary support or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery." 37 CFR 11.18(b)(2)(iii). Moreover, *In re Wyer*, 655 F.2d 221 (C.C.P.A. 1980) (cited by Patent Owner) holds only that "sufficient proof" as to the publication date must exist. *Id.* at 226-27. No authority supports Patent Owner's contention that Requestor was required to present evidence of the date of public availability of each reference with the Request. Regardless, evidence was presented with the Request that unequivocally establishes that each of *Aventail, BinGO!, Kent*, *Reed*, *Wang* and the RFC documents was publicly disseminated before February 15, 2000, and is thus prior art to the '135 patent.[1]

The three *Aventail* publications were publicly disseminated with deployments of Aventail products no later than August 9, 1999. Submitted with the Request were three separate declarations, each of which documented how each *Aventail* publication was made available to the public, and demonstrated that each had been made available no later than August 9, 1999. Patent Owner ignores this evidence, contending there is no "corroborative evidence" demonstrating public

---

[1] Patent Owner does not contest Requester's assertions on page 10 of the Request that the effective filing date of the '135 patent was no earlier than February 15, 2000.

availability. Patent Owner, however, ignores the fact that the declarations corroborate themselves. Indeed, there is remarkable consistency in the testimony of Mssrs. Hopen, Fratto, and Chester about the dates when the *Aventail* publications were publicly disseminated which conclusively establishes that the *Aventail* publications were publicly disseminated before February 15, 2000.

The *BinGO!* publication (i.e., the *BinGO! User Guide* ("*BinGO! UG*") and *BinGO!Extended Feature Release* ("*BinGO! EFR*")) was publicly disseminated no later than April 17, 1999. As explained in the Request, these documents on their face disclose publication dates well before February 15, 2000. *BinGO! UG*, for example, has a March 1999 copyright date, and *BinGO! EFR* indicates it was published one month earlier. Despite this, Patent Owner asserts that these dates are "merely evidence of creation, not of publication or dissemination" and "Without more, this unsupported assertion of the alleged copyright date of the document as the publication date does not meet the 'publication' standard required for a document to be relied upon as prior art." Response at 7-8. As established in Exhibit A (Affidavit of Christopher Butler), the *BinGO!* documents were distributed on the Internet no later than April 17, 1999, which is shown, *inter alia*, by entries in the Internet Archive ("the Wayback Machine") of that date. As provided in M.P.E.P. § 2128, "[a]n electronic publication, including an on-line database or Internet publication, is considered to be a 'printed publication' within the meaning of 35 U.S.C. 102(a) and (b) provided the publication was accessible to persons concerned with the art to which the document relates."

The *Reed* paper was formally published as part of a compilation of technical papers that were originally presented to conferences of experts in network and security techniques. Specifically, *Reed* indicates that it was distributed to the public at the 12th Annual Computer Security Applications Conference (ACSA) as early as December 1996, and was subsequently published in "ACSAC '96 Proceedings of the 12th Annual Computer Security Applications Conference" (ISBN:0-8186-7606-X). Patent Owner does not seriously contest these facts. Instead, Patent Owner simply contends Requester did not present additional evidence with the Request proving these statements were true. Requester had no such burden. Nonetheless, Requester presents additional evidence in the Second Declaration of Michael Fratto ("Fratto 2d") establishing that *Reed* was formally published and distributed well before February 15, 2000. *See, e.g.,* Fratto 2d at ¶¶ 8-13. Thus, *Reed* is a printed publication that was made publicly available no later than December of 1996. *See e.g., In re Bayer*, 568 F.2d 1357, 1361 (C.C. P.A.1978).

Wang indicates on its face that it was made publicly available as of September 16, 1999. According to the document, Broadband Technical Reports "may be copied, downloaded, stored on

a server or otherwise re-distributed in their entirety. . .” *Wang* at 2. As Mr. Fratto explains, the Broadband Forum maintains public access to technical reports via their website, including documents dating back to 1996. Fratto 2d at ¶14. Thus, *Wang* is a printed publication that was made publically available before February 15, 2000.

Patent Owner next challenges the status of the Request for Comment (RFC) documents cited in the Request, claiming that “the record is devoid of evidence that any of these references are … printed publications as of” each publication date listed on each RFC. This is a frivolous challenge – RFC documents are published and disseminated to the public by the Internet Engineering Task Force (IETF) pursuant to transparent and well-known procedures. Specifically: (i) each number assigned to an RFC is unique and is not “re-used” if the subject matter in an RFC is revised or updated, (ii) the date each RFC is distributed to the public is listed the front page of the RFC, (iii) RFCs are distributed to the public over the Internet, via numerous protocols, (iv) each RFC is announced via an email distribution list on the date it is released to the public, and (v) RFCs are maintained in numerous archives publicly accessible via the Internet. *See* Fratto 2d at ¶18-22. In fact, Patent Owner itself cites several RFCs as “printed publications” in the ‘135 patent. Patent Owner thus cannot seriously contend that RFCs are not publicly disseminated.[2]

III. The Rejections Of the Claims Were Proper And Should Be Maintained

Claims are given “their broadest reasonable interpretation, consistent with the specification, in reexamination proceedings.” *In re Trans Texas Holding Corp.*, 498 F.3d 1290, 1298 (Fed. Cir. 2007). In determining that meaning “it is improper to ‘confin[e] the claims to th[e] embodiments’ found in the specification.” *Id.* at 1299 (quoting *Phillips v. AWH Corp.,* 415 F.3d 1303, 1323 (Fed. Cir. 2005) (*en banc*)). While “the specification [should be used] to interpret the meaning of a claim,” the PTO cannot “import[] limitations from the specification into the claim.” *Id.* “A patentee may act as its own lexicographer and assign to a term a unique definition that is different from its ordinary and customary meaning; however, a patentee must *clearly* express that intent in the written description.” *Helmsderfer v. Bobrick Washroom Equip., Inc.*, 527 F.3d 1379, 1381 (Fed. Cir. 2008) (emphasis added). No such express definitions of key claim terms is provided in the ’135 patent (e.g, “virtual private network,” “transparently creating a virtual private network,” “domain name service,” “secure web site,” “determining,” or “between.”) Thus, these terms must be given their broadest reasonable interpretation in these reexamination proceedings.

---

[2] *See, e.g.,* ’135 Reexam Certificate at 5.

A. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1, 3, 4, 6-10 and 12-14 Under 35 U.S.C. § 102(a) Based on *Aventail Connect v3.1/2.6 Administrator's Guide* (Issue No. 1)

1. Independent Claim 1 (Issue No. 1)

As explained in the Request, *Aventail* describes a system that automatically establishes a Virtual Private Network ("VPN") in response to a determination that a DNS request made on a client computer is requesting access to a secure target computer. Request at 38-57. Consequently, the Office properly found that *Aventail* describes a system that anticipates claim 1. OA at 9. In response, Patent Owner asserts *Aventail* does not teach a system that is: (1) "arranged or combined in the same way as recited in the claim"; (2) "disclose[s] a VPN" or (3) "automatically initiat[es] a VPN in response to determining that a DNS request is requesting access to a secure target web site." Response at 25. Each of these is incorrect.

a. *Aventail* Describes A System Arranged In the Same Manner as Recited in the Claim.

As explained in the Request, *Aventail* describes a system that "generat[es] from the client computer a Domain Name Service (DNS) request," "determin[es] whether the DNS request . . . is requesting access to a secure web site"; and "automatically intiat[es] the VPN between the client computer and the target computer." *See, e.g.,* Request at 38-57. In response, Patent Owner asserts that even if these elements are disclosed in *Aventail*, they are not "arranged or combined in the same was as recited in the claim."[3] Response at 19-20. Patent Owner's response should be disregarded for the simple fact that claim 1 simply recites a process "comprising" a number of recited steps – it does not impose the strict order imagined by the Patent Owner.

More importantly, however, *Aventail* does describe a system that performs the steps recited in the order they are recited in claim 1 to automatically establishes a VPN in response to a determination that a DNS request is requesting access to a secure website. Specifically, *Aventail* shows systems that intercept and evaluate DNS requests, determine if they are requesting access to a secure destination, and, if so, automatically authenticate and encrypt communications between the client computer and a private network resource via a VPN server called the Aventail Extranet Server. Fratto at ¶87. Aventail Connect worked with applications that communicate via TCP/IP—

[3] Patent Owner incorrectly asserts that *Aventail* distinguishes between "outbound" and "inbound" access. The two terms are simply a function of perspective – an "outbound" request from a client computer for access to a secure target computer would, from the perspective of the secure target computer, be an "inbound" connection.

such as Web browsers—and was implemented using the existing WinSock functionality in client computers running Windows. Fratto at ¶89. Thus, Aventail Connect necessarily acted on DNS requests containing, for example, either hostnames or IP address. *Id.* ("[Aventail Connect] executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address."), and evaluated such requests to determine if the request was seeking access to a destination that required authentication and encryption, such as a secure website, or access to a non-secure destination, such as a public website on the Internet. Fratto at ¶91. If Aventail Connect determined that a DNS request contained a hostname specifying a secure destination inside a private network, it would automatically and transparently (i) handle authentication of the user to the private network and (ii) encrypt the communications between the client computer and the private network resource, thereby establishing a VPN. Fratto at ¶91. Thus, as described in the '135 patent, *Aventail* discloses a system that automatically establishes a Virtual Private Network ("VPN") in response to a determination that a DNS request made on a client computer is requesting access to a secure computer.

In response, Patent Owner argues (incorrectly) "the Request casually moves between and picks certain features from various different embodiments in an attempt to satisfy the elements of claim 1." Response at 20. Patent Owner's stylistic criticism is irrelevant, and its substantive comments are simply wrong. In fact, it is Patent Owner that misrepresents key teachings of *Aventail*. For example, Patent Owner incorrectly states that the Request "briefly refers to an embodiment of *Aventail v3.1* dealing with inbound connections to show that web pages behind an Aventail ExtraNet server may be accessed by a web browser," and then "refers back to the originally cited outbound embodiment." Response at 19. Yet, the section to which Patent Owner refers unambiguously describes configuring a web browser on a client computer so that Aventail Connect can appropriately redirect "connections through the outbound proxy." *Aventail Connect v3.1* at 74 (emphasis added). Thus, *Aventail* shows configuring Aventail Connect for use with a web browser to appropriately route outbound traffic destined for "those sites that are protected in the secure extranet." *Id.*

b. *Aventail* Discloses a VPN

The Examiner correctly found that *Aventail* discloses "automatically initiating the VPN between the client computer and target computer." In response, Patent Owner asserts that *Aventail* does not disclose a VPN because "[o]ther than an unreferenced drawing of a 'VPN server,' the

term 'VPN' is not used in *Aventail v3.1* to describe any connection." Response at 21. Patent Owner assertions are incorrect.

As Patent Owner readily admits (Response at 21), *Aventail* explicitly discloses a "VPN Server." The VPN Server in *Aventail* (i.e., the Aventail ExtraNet Server) is described as working in conjunction with Aventail Connect client to establish encrypted communications over the Internet between a client computer and a secure destination on a private network. *See, e.g.,* Request at 42. A person of ordinary skill would plainly understand from this description that *Aventail* is describing a VPN. *See* Fratto ¶116-118 ("[P]eople used 'VPN' to refer to a group of networking protocols and techniques that enabled a remote user to securely gain access to one or more resources available on a private network via a public network, such as the Internet.").

The Patent Owner contends that *Aventail* does not disclose a VPN because the encrypted communication tunnel disclosed in *Aventail* fails to satisfy the definition of a VPN according to testimony from its expert in a prior reexamination. Response at 21-22. That expert –Jason Nieh – asserted that (1) "*Aventail v3.1* has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network," (2) "Aventail Connect's fundamental operation is incompatible with users transmitting data that is sensitive to network information," and (3) "computers connected according to *Aventail v3.1* do not communicate directly with each other." Response at 21-23. Patent Owner's analysis and its expert's dated declaration are legally irrelevant and factually incorrect.

Contrary to Patent Owner's assertions, the claims do not require the specified functionalities. Specifically, the term "virtual private network" is not expressly defined in the claims or the specification to require these functionalities. Thus, the claims do not require a VPN that enables computers to communicate "as though they were on the same network" or computers that are "communicating directly with each other." Patent Owner also provides nothing to support its assertions that the "fundamental operation" of the *Aventail* systems is "incompatible with users transmitting data that is sensitive to network information." To the contrary, *Aventail* plainly shows systems that securely transmit – using encryption and other techniques – information to enable remote users to securely access secure resources on a private network.

Patent Owner's assertion about the functionality of the *Aventail* systems also is incorrect. For example, *Aventail* plainly shows remote users being able to access private network resources using the "Extranet Neighborhood" functionality of the *Aventail* system. *See Aventail* at 28-30, 95-100. Thus, *Aventail* does describe systems where remote users can communicate "as if they were

on the same network" and can communicate "directly with other users" on the network. Similarly, Patent Owner's incorrectly describes how the Aventail Connect client functions, claiming that the "false DNS response" returned by the Aventail Connect client if a DNS request is determined to specify a secure destination will "prevent the correct transfer of data." Response at 22. In fact, as *Aventail* clearly explains, the Aventail Connect client uses the "false DNS entry" to simply flag DNS requests specifying secure destinations (i.e., hostnames matching a redirection rule). Once flagged, those requests are redirected to the Extranet Server, which performs the required authentication and encryption steps, and establishes the VPN. Fratto at ¶ 63. The false network information is never used as an actual network destination, a conclusion that is inescapable from the description in *Aventail*. Thus, contrary to Patent Owner's assertion, the "false DNS response" is used to facilitate, not prevent, the secure transfer of data through a VPN.

c. *Aventail* Discloses the "Automatically Initiating a VPN" Step

The Examiner correctly found that the *Aventail* publications disclose a system that "automatically initiat[es] a VPN in Response to Determining that a DNS request is determined to be requesting access to a secure web site." As the Request explains, *Aventail* shows that a client computer running Aventail Connect will determine if a DNS request transmitted by an application on the client computer is requesting access to a destination requiring a VPN. *Aventail Connect* at 10 ("When the Aventail Connect [] receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack.").

In response, Patent Owner contends that "the Request does not say how a DNS request is determined to be requesting access to a secure website." This response simply ignores the contents of *Aventail*, which clearly explains that if a client computer running Aventail Connect determined that a DNS request matched a redirection rule requiring a VPN (e.g., if the hostname in the request is identified as "part of a domain we are proxying traffic to"), the computer running Aventail Connect initiates the steps necessary to automatically establish a VPN to access the secure destination located on the specified private network. Request at 40-41; *see also* Fratto ¶ 61-70. These steps include determining if the connection request specified a destination on a pre-defined list of secure destinations, and if so, depending on the configuration of the client, sending the connection request to Aventail ExtraNet Server, which would authenticate the user, define the

encryption technique to be used, and otherwise determine whether and how traffic destined for a private network resource will be proxied. Request at 40-42; *see also* Fratto ¶ 100-101.

Notably, the Patent Owner and its expert do not argue that the sequence of steps shown in *Aventail* do not meet the requirements of the claim. Instead, their response claims that each step considered in isolation does not anticipate the claims (i.e., none of the steps individually constitute the "determination" step of the claims). For example, Patent Owner argues that "the mere existence of a 'security policy' or 'configuration' of a server in *Aventail v3.1* does not involving *determining* whether any request, must less the claimed DNS request, is requesting access to a secure web site, as recited in claim 1." Response at 23. The Request did not contend that the configuration files on the ExtraNet Server alone anticipated this element of claim 1. Instead, the Request pointed to the description in *Aventail* showing how client computers running Aventail Connect working with the Extranet Server performed the determination step in a variety of ways. And plainly *Aventail* does show the determination step of claim 1.

Similarly, Patent Owner argues that "the Request also cannot properly contend that evaluating the connection request for the presence of a false DNS entry discloses determining that a DNS request is requesting access to a secure target web site." Response at 24. This analysis is refuted by the plain teachings in *Aventail*. As explained in the Request, the Aventail Connect client would determine if a connection request was seeking access to a secure resource or not. If it was, and contained a domain name, a "false" DNS entry would be used to flag that connection request as requiring handling according to the policies enforced by the ExtraNet Server. Request at 40-42. The "determining step" thus begins before the false DNS entry data introduced by the Aventail Connect client activity is used to re-direct the connection request and begin the process of establishing the VPN.

Patent Owner also contends that *Aventail* "does not disclose that encryption (*i.e.,* the purported VPN) is automatically initiated in response to determining that the DNS request in step (2) is requesting access to a secure target web site," and that no "link between the alleged *DNS request* and the encryption, much less that it is automatically initiated in response to determining that a DNS request in step (2) is requesting access to a secure target web site, as recited by claim 1." Response at 24-25. Both assertions are incorrect. As explained in the Request and demonstrated above, *Aventail* shows a VPN being automatically established between a client computer running an Aventail client and a destination computer, after it is determined that the connection request has specified a secure resource (i.e., the destination computer) on a private

network. If it does, the client computer running the Aventail client performs the authentication of the client with the VPN Server. If that authentication is successful, the Aventail VPN Server then establishes the VPN automatically with the destination specified in the DNS request. *Aventail* at 42 ("Aventail can establish an encrypted tunnel automatically.") Thus, encrypted network traffic is sent between the client and secure destination over the Internet, and the Aventail client and ExtraNet server automatically encrypt outgoing and decrypts incoming traffic. Request at 42-44. Fratto ¶ 88-89, 94, 97-98, 100-105.

Patent Owner also incorrectly contends that the sending of "the hostname to a DNS server on another computer for resolution" is what "the Request contends discloses a DNS request." Response at 24. The Patent Owner then points to a series of steps that occurs subsequent to the request in order to conclude that "what the Request points to as the request for an IP address is generated by Aventail Connect (from the client computer) after the establishment of what the Request points to as the VPN." Response at 25. The Patent Owner has apparently confused the resolution of the DNS request with the connection request itself. As the Request explained, Aventail Connect worked with applications that communicate via TCP/IP, and was implemented using the WinSock functionality in client computers running Windows. Request at 38-40. Windows TCP/IP networking applications (such as telnet, e-mail, Web browsers, and ftp) use WinSock to gain access to networks or the Internet. This meant that Aventail Connect would act on connection requests generated on the client computer (e.g., a connection request from a web browser), which could contain either a hostname or an IP address. Request at 38-40. Fratto ¶ 88-90. If the connection request contained a domain name requiring resolution into an IP address, *Aventail* explains that the Aventail Connect software running on the client computer would intercept the DNS request, evaluate it, and, as appropriate, either resolve it into an IP address or pass it off for handling by the ExtraNet Server. In other words, once the Aventail Connect client determined – either based on the domain name or the IP address in the connection request – that the request was specifying a secure destination (e.g., it matched an entry on a list of secure destinations), it would establish a connection to the Extranet Server, authenticate the client and establish the secure tunnel, all of which would be transparent to the user. Thus, *Aventail* describes a system that automatically establishes a VPN in response to a determination that a DNS request made on a client computer is requesting access to a secure computer. The Examiner's finding of anticipation of claim 1, thus, should be maintained.

2. Dependent Claims 3, 7, 12 (Issue No. 1)

The Examiner correctly found that *Aventail* discloses every limitation of dependent claims 3, 7, and 10. In response, Patent Owner argues only that these claims "are patentable for at least reasons similar to those discussed" in their respective independent claims. Response at 26-28. Because no independent reasons were presented by Patent Owner regarding claims 3, 7 and 12, the rejection of these claims based on *Aventail* should be maintained.

3. Dependent Claim 4 (Issue No. 1)

The Examiner correctly found that *Aventail* discloses every limitation of dependent claim 4. In response, Patent Owner and its expert assert that "the [Aventail] server does not even attempt to resolve a hostname until after the client computer is authenticated."[4] This is plainly incorrect. *Aventail* shows systems that, in one embodiment, comprise a client computer running Aventail Connect that intercepts connection requests, determines if the request is seeking access to a secure destination, and if so, determine if the user is authorized to access the secure destination, before establishing the VPN (alone or in conjunction with the Extranet Server). *See, e.g.,* Request at 44. The Request also explains (supported by testimony from several experts) that *Aventail* shows systems that "would inherently know how to handle errors returned according to the relevant DNS and TCP/IP communication protocols." Moreover, nothing in claim 4 requires the error to be returned after a DNS resolution step. As explained in the Request, when a "DNS request is unsuccessful, the address record returned in the response will not contain the resolved IP address, but instead will contain an RCODE," and such response would be inherent in the "Aventail VPN solutions." Request at 47; Fratto ¶ 140-142. Consequently, the Examiner's rejection of this claim as anticipated by *Aventail* was also proper and should be maintained.

4. Dependent Claim 6 (Issue No. 1)

The Examiner correctly found that *Aventail* discloses every limitation of dependent claim 6. In response, Patent Owner again asserts the Examiner cannot rely on the declaration evidence of record without formally incorporating by evidence in the Office Action. Response at 27. There is no such requirement in law or PTO rules. Next, Patent Owner asserts "the declaration does nothing to show that a VPN is established by creating an IP address hopping scheme," because the disclosed "proxy schemes [in *Aventail*] are implemented merely to satisfy the 'need to traverse

[4] Patent Owner contends rejection is improper because the declarations provided with the Request "were not incorporated by reference [and] are not relied upon for the rejections presented in [the] Office Action." This assertion can be simply ignored – there is no requirement for an Examiner to "incorporate by reference" the evidence of record in a reexamination proceeding.

multiple firewalls.'" Response at 27. The Patent Owner concludes that "providing a mechanism for traversing multiple firewalls does not contribute in any meaningful way towards securing data transmitted over a public network, much less establishing a VPN." Response at 27. The Patent Owner's statements are irrelevant – nothing in the claims require the IP address hopping scheme to contribute "in any meaningful way towards securing data." More directly, the IP hopping schemes described in *Aventail* obviously do "meaningfully contribute" to securing the data being transmitted – they help maintain the privacy of an encrypted tunnel between a client computer and secure target destination. Patent Owner's comments thus rest on assumptions that are both irrelevant and technically incorrect. Accordingly, the Examiner's rejection of claim 6 was proper and should be maintained.

5. Dependent Claim 8 (Issue No. 1)

The Examiner correctly found that *Aventail* discloses every limitation of dependent claim 8. In response, Patent Owner contends that the Office Action has not met its burden of "show[ing] that a client computer, including the TCP/IP stack, as described by *Aventail*, can be seen as a DNS server." Response at 28. Patent Owner's response is meritless – the Office Action expressly references portions of the Request, including those portions that explain how Aventail Connect passes through the DNS query to the TCP/IP stack for resolution on the local workstation. Request at 51-52 ("If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running."). Thus, the Examiner's rejection of claim 8 was proper and should be maintained.

6. Independent Claim 10 (Issue No. 1)

Aventail describes a system including a DNS proxy server that establishes a VPN in response to a determination that a DNS request made on a client computer is requesting access to a secure computer, together with a gateway computer that allocates resources for the VPN. See Request at 52-55. Consequently, the Office properly found that *Aventail* anticipates claim 10. OA at 9. In response, Patent Owner asserts that (1) "Aventail Connect cannot be construed as a DNS proxy server;" (2) *Aventail* "does not disclose the feature of a DNS proxy server that generates a request to create a VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested;" and (3) *Aventail* "does not disclose the feature of a gatekeeper computer that allocates resources for the VPN between the

client computer and the secure web computer." Response at 29-31. Each of these is incorrect.

a. *Aventail* Discloses a DNS Proxy Server that Returns an IP Address for DNS Requests Not Specifying Secure Destinations

The Examiner correctly found that Aventail Connect is a DNS Proxy Server within the meaning of claim 10. As the Request explains, *Aventail* shows client computers running Aventail Connect configured to handle DNS resolution locally (on the client computer) or to send the DNS requests to a different computer (the Aventail Extranet Server) for resolution. Request at 53. Either embodiment shows a DNS proxy server (e.g., a client computer running Aventail Connect in conjunction with the Windows OS or the Extranet Server) which receives a DNS request and in response, either returns an IP address to the requesting application the hostname or IP address in the DNS does not specify a secure destination, or automatically establishes a VPN if the request specifies a secure destination. Request at 54. Specifically, *Aventail* shows that if the DNS request included a hostname that did not match a destination specified in a redirection rule (*i.e.*, because the destination did not require a VPN), then either the Aventail Connect client alone (*e.g.*, where the name matches a local resolution rule in the Aventail configuration) or Aventail Connect working in conjunction with the operating system of the client computer (*i.e.*, WinSock and the TCP/IP stack on a Windows computer) would resolve the request to yield an IP address. Request at 53. In response, Patent Owner incorrectly asserts that the *Aventail* "does not establish disclosure of a DNS proxy server that returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested." To make this assertion, Patent Owner simply ignores the relevant disclosures in *Aventail*. In addition, Patent Owner resorts to an illogical and strained reading of *Aventail* to conclude that Aventail Connect working in conjunction with the operating system of the client computer (a computer) is not a DNS proxy server, ignoring that the disclosure of the '135 patent expressly states that the DNS proxy server can be a "computer or a program." Response at 29. Moreover, the claims impose no additional requirements on the "DNS Proxy Server." Thus, contrary to Patent Owner's assertions, *Aventail* discloses a DNS proxy server meeting the requirements of claim 10.

b. *Aventail* Discloses a DNS Proxy Server that Automatically Establishes VPNs with Secure Destinations

The Examiner properly found that *Aventail* discloses a DNS Proxy Server that establishes a VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested (and the user is properly authenticated). Patent Owner

disagrees, contending that *Aventail* shows this "is performed only when 'the request contains a routable IP address," and thus the purported proxy server would not receive a request from the client computer to look up an IP address from which a determination may be made." Response at 30. The Patent Owner is simply wrong on both accounts. As the Request explains, if a client computer running Aventail Connect determined that a DNS request contains a domain name matching a redirection rule requiring a VPN (e.g., if the hostname in the request is "part of a domain we are proxying traffic to"), then Aventail Connect would initiate the steps necessary to automatically establish a VPN to the secure destination on the private network. Request at 40-41; Fratto ¶61-70. In particular, *Aventail* shows steps that include verifying the security policies based on configuration of the Aventail ExtraNet Server (defining whether and how traffic destined for a private network resource is to be proxied), handling authentication, and automatically encrypting/decrypting the traffic sent and received from the VPN server. Request at 40-42; Fratto ¶ 100-101. To conclude otherwise, Patent Owner again improperly analyzes the steps in *Aventail* in isolation, contending that each individually fails to "generate[s] a request to create a VPN" requirement of the claims, and then ignores the actual teachings of *Aventail*.

c. *Aventail* Discloses a Gatekeeper Computer that Allocates Resources for the VPN Between the Client Computer and the Secure Web Computer

The Examiner found that *Aventail* discloses a "gateway computer" as described in the claims. In response, Patent Owner alleges only that Aventail does not disclose a VPN. For the same reasons discussed above in section A(1)(b), the Patent Owner is incorrect. Thus, the Examiner's finding of anticipation of claim 10 was proper and should be maintained.

7. Independent Claim 13 (Issue No. 1)

The Request explains how *Aventail* describes a system including "establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers." Request at 55-56. The Office consequently found that *Aventail* describes a system that anticipates claim 13. OA at 9. In response, Patent Owner asserts that *Aventail* does not disclose a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers" and "authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client." Response at 31. Patent Owner is again incorrect.

Aventail describes systems where multiple clients running Aventail Connect communicate with an Aventail VPN Server, and, if successfully authenticated, work with the VPN Server to establish a VPN between the client computer and a secure destination computer. As Patent Owner concedes, *Aventail* discloses that "the Aventail ExtraNet Server require[s] all users to use Aventail Connect to authenticate and encrypt their sessions." Response at 32. *Aventail* further discloses organizing data in a manner that correlates client computer information to credential information, and thus satisfies the requirement of claim 13 to maintain a plurality of authentication tables each corresponding to one of the client computers. Request at 56. Moreover, because *Aventail* systems require each client computer present authentication credentials in order to establish a VPN, the *Aventail* system necessarily comprise authentication tables in order to validate those credentials. Request at 55-56; Fratto ¶ 178-87. Consequently, the Examiner's rejection of this claim as anticipated by *Aventail* was proper and should be maintained.

8. Dependent Claim 14 (Issue No. 1)

The Examiner correctly found that *Aventail* discloses every limitation of claim 14. In response, Patent Owner contends "the declarations submitted by the Requester were not relied upon by the Office Action." Response at 33. For reasons presented above, Patent Owner is incorrect—the declarations are evidence of record, and the Examiner need not "incorporate" or "officially notice" them to support a finding of anticipation. Response at 33. Patent Owner next contends that the Request "does not disclose how IP header information would be altered." Response at 33. This assertion, unsupported by any evidence, is simply wrong. The Request explains that *Aventail* discloses both MultiProxy and Proxy Chaining schemes that route VPN IP traffic between the client and secure target computers. These techniques redirect network traffic via techniques in which changes are made to "at least one field" in a series of data packets being sent between the client and target computers. In particular, under either technique, the IP header information must be altered to change the destination and/or the origination data fields in the packets to effect the re-routing of the traffic through the intermediary proxy servers. Request at 56-57. The MultiProxy and Proxy Chaining schemes thus necessarily perform an "alteration of IP header information" as an inherent step in re-routing TCP/IP packets under standardized protocols. Accordingly, the Examiner's rejection of this claim was proper

B. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1, 3, 4, 6-10 and 12-14 Under 35 U.S.C. § 102(b) Based on *Aventail Connect v3.01/2.51 Administrator's Guide* (Issue No. 2)

The Patent Owner does not challenge any of the evidence or explanations in the Request that are specific to *Aventail Connect v.3.01/Administrator's Guide*, but instead incorporates and relies on its positions stated with respect to *Aventail v3.1/Administrator's Guide*. Consequently, for the reasons presented above, the Examiner's rejection of these claims as anticipated by *Aventail v3.01/Administrator's Guide* was proper and should be maintained.

C. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1, 3, 4, 6-10 and 13 Under 35 U.S.C. § 102(b) Based on *Aventail AutoSOCKS Administrator's Guide* (Issue No. 3)

The Patent Owner does not challenge any of the evidence or explanations in the Request that is specific to *AutoSOCKS/Administrator's Guide*, but instead incorporates and relies on its positions stated with respect to *Aventail v3.1/Administrator's Guide*. Consequently, for the same reasons demonstrated above by Requester, the Examiner's rejection of these claims as anticipated by *AutoSOCKS/Administrator's Guide* was proper and should be maintained.

D. Response to Patent Owner's Arguments Regarding the Rejection of Claim 11 Based on *Aventail v3.1*, in View of *Reed and Goldschlag* (Issue No. 4)

The Request explains that *Aventail* in view of *Reed* would have rendered obvious to a person of ordinary skill a system whereby a "gatekeeper computer creates the VPN by establishing an IP address hopping regime that is use to pseudorandomly change IP addresses in packets transmitted between the client computer and the secure target computer." Request at 107-109. The Office properly rejected claim 11 on this basis. OA at 9. In response, Patent Owner asserts (1) "*Reed* has not been shown to disclose an IP address hopping regime and (2) "*Aventail v3.1* cannot be combined with *Reed*." Response at 35-37. Each of these is incorrect.[5]

1. *Reed* Discloses an "IP Address Hopping Regime"

The Examiner correctly found that *Reed* discloses an "IP address hopping regime" within the meaning of claim 11, and that *Aventail* in view of *Reed* would have rendered Claim 11 obvious. As the Request explains, *Reed* discloses "IP hopping regimes that pseudorandomly change IP addresses in packets transmitted between" an originating and destination computer. Request at 108-109; Fratto at ¶¶ 167-174. The *Reed* onion-routing schemes thus are "IP hopping" schemes – they route IP packets via intermediate destinations to a final destination. These schemes also "pseudorandomly" change IP addresses because they route the IP traffic according to schemes that

[5] The Patent Owner again incorrectly asserts that the declaration evidence should be ignored because the Examiner did not incorporate them into the Office Action.

appear random without knowledge of the order of routing specified by the onion routers. Request at 108-09. Finally, the onion-routing schemes disclosed in *Reed* work by changing IP addresses in packets transmitted between the origination and destination computers. Request at 108-09.

In response, Patent Owner contends – disingenuously – that *Reed* does not disclose "IP Addresses," asserting "there is no mention of 'IP address" in *Reed,* let alone any description in *Reed* that an IP address is necessary for the operation of the onion routing." Response at 35-36. It is only by studied ignorance of *Reed* that the Patent Owner could conclude that this paper does not disclose operations performed on packets containing IP addresses. *Reed* plainly describes integration of onion-routers in systems where TCP/IP packets are being sent, routed and received (e.g., by Web browsers, remote login, and email). TCP/IP packets, according to the well-established TCP/IP protocol, contain IP addresses. *Reed*, thus, necessarily teaches IP hopping schemes which function by "pseudorandomly" changing IP addresses in packets transmitted between an originating and destination computer.

2. A Person of Ordinary Skill Would Find Motivation in *Aventail* to Modify the VPN Processes Disclosed Therein to Incorporate *Reed*

The Examiner correctly rejected claim 11 as being obvious over *Aventail* in view of *Reed* because a person of ordinary skill in the art would have found a motivation within *Aventail* to incorporate onion-routing schemes taught by *Reed* as an additional security measure to prevent the monitoring of networking traffic in the *Aventail* systems. Patent Owner disagrees, asserting that *Aventail* "would not be understood to be applicable to third-parties attempting to monitor traffic flowing in our out of a firewall, or between the firewall and some remote location," and that "[t]o the contrary, *Reed* teaches how to prevent the monitoring of network usage." Response at 36.

As explained in the Request, a person of ordinary skill in the art would find motivation within *Aventail* to modify the VPN processes and systems disclosed therein to incorporate additional mechanisms to prevent the monitoring of networking traffic. Request at 108-09. That person also would find in *Reed* identification of the same problem (prevent network monitoring), as well as a solution to that problem; a particular type of an "IP hopping scheme" (onion-routing). Request at 108-09. Claim 11, which differs from the systems described in *Aventail* solely with respect to the "pseudorandom" IP hopping scheme element, thus, would have been obvious to a person of ordinary skill in the art in view of *Aventail* in view of *Reed*.

3. *Aventail v3.1*, in View of *Reed,* in Further View of *Goldschlag*, Renders Claim 11 Obvious (Issue No. 4)

The Examiner correctly found that *Aventail*, in view of *Reed*, and further in view of *Goldschlag*, discloses an "IP address hopping regime" that "pseudorandomly change IP addresses in packets" within the meaning of claim 11. As the Request demonstrates, *Reed* discloses an "IP hopping regimes that pseudorandomly change IP addresses in packets transmitted between" an originating and destination computer. Request at 108-109; Fratto at ¶¶ 167-174. The Request also cited *Goldschlag* as further evidence that the *Reed* onion routing method uses an initiator's proxy to change the routing of an IP packet sent from an originating computer to go through a series of onion-routers that are intermediary destinations. The IP packets, thus, are necessarily changed in a "pseudorandom" manner incidental to the process of re-routing those packets. Request at 104.

Patent Owner disagrees, asserting that the Office has not shown the pertinence of *Goldschlag* to claim 11. Response at 38. Patent Owner simply ignores that the Examiner adopted the statements of the Requester, which explain how *Goldschlag* relates to claim 11. Patent Owner argues in the alternative that *Goldschlag* "merely hypothesizes that nodes may be instructed to 'choose their own route.'" Response at 39. It is immaterial whether the systems described in *Goldschlag* were ever deployed – *Goldschlag* clearly describes these techniques, which makes *Goldschlag* prior art to claim 11. Patent Owner also asserts that *Goldschlag* does not satisfy the claim because it specifies that "nodes [] choose their own route," so "the route chosen by a node may be predetermined." Response at 39. However, neither the claims nor the specification attach a special meaning to "pseudorandom" as used in the claims. Patent Owner's assertions that the claims are limited to one particular form of a "pseudorandom" re-routing technique must thus be disregarded, as claim 11 encompasses an IP-hopping scheme that routes IP packets pursuant to a pre-determined hopping path. Consequently, the Examiner's rejection of this claim was proper.

E. Response to Patent Owner's Arguments Regarding the Rejection of Claim 11 Under 35 U.S.C. 103 Based on *Aventail v3.01* in View of *Reed* (Issue 5)

Patent Owner presents no distinct response to the rejection of claim 11 based on *Aventail v3.01* in view of *Reed* relative to its response to the rejection of this claim based on *Aventail v3.1* in view of *Reed*. Thus, for the reasons noted above, the Examiner's rejection of the claims based on *Aventail v3.01* in view of *Reed* was also proper and should be maintained.

F. Response to Patent Owner's Arguments Regarding the Rejection of Claim 11, 14, & 15 Under 35 U.S.C. 103 Based on *AutoSOCKS* in View of *Reed* (Issue 6)

1. Dependent Claim 11

Patent Owner presents no distinct response to the rejection of claim 11 based on *AutoSOCKS* in view of *Reed* relative to its response to the rejection of this claim based on *Aventail 3.1* in view of *Reed*. Consequently, for the reasons noted above, the Examiner's rejection of claim 11 based on *AutoSOCKS* in view of *Reed* was also proper and should be maintained.

2. Dependent Claim 14

The Examiner correctly found that *AutoSOCKS* in view of *Reed* renders obvious dependent claim 14. In response, Patent Owner provides a contorted interpretation of the observations in the Request regarding the role of the Aventail ExtraNet Server in establishing VPNs as taught by *AutoSOCKS*, and on that basis asserts that claim 14 would not have been considered obvious.

Claim 14 differs from claim 13 by its inclusion of the step of communicating "according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence." As explained in the Request at page 113, including this step in the communications systems taught by *AutoSOCKS* would have been obvious to a person of ordinary skill in the art based on *Reed*. In particular, *Reed* teaches the onion routing technique in which IP addresses in TCP/IP packets are periodically changed according to a known sequence. This technique is described by *Reed* to as being useful for preventing the interception or monitoring of TCP/IP network traffic on the Internet. *Reed* at 1-2. *Reed* further explains this technique can be integrated into systems that employ TCP/IP communications. A person of ordinary skill in the art considering *AutoSOCKS* would recognize both the benefit of including this technique to enhance the security of communications over the Internet and that it would be compatible with the *AutoSOCKS* solution because the latter is communicates via TCP/IP communications.

Patent Owner next asserts the ExtraNet Server shown in *AutoSOCKS* is not a "central computer" and criticizes the Request for portraying onion-routers as "second computers" according to claim 13. In particular, Patent Owner contends that Requestor "shifts its previous arguments to reflect that a second computer is no longer seen as a destination computer or remote host." Patent Owner's comments border on the nonsensical. First, the explanation at page 113 of the Request did not claim only that onion-routers in *Reed* were "second computers."[6] Instead, it pointed out that an onion-router could be a "second computer" according to the broad language of claims 13 and 14. More importantly, as the comments on page 113 make clear, a person of ordinary skill in the art would have considered it to be obvious to incorporate the onion-routing schemes taught by

[6] The use of the term "i.e.," in referring to onion-routers as second computers appears to have been a typographical error in the Request. The correct modifier should have been "e.g.".

Reed into the secure communication systems taught by *AutoSOCKS*, in which second computers plainly may be computers on the private network. As *AutoSOCKS* teaches, the ExtraNet Server mediates establishment of a VPN, acts as the "central computer" of claim 13, and provides access to computers on the private network by working in conjunction with client computers running AutoSOCKS client software. The onion-routing schemes taught by *Reed* change at least one field in the data packets by taking an incoming IP packet and incorporating its contents into an onion data structure that adds origination and destination IP addresses as the onion data packet is routed through intermediary onion routers to the second computer, i.e., the secure destination computer. Request at 113. Patent Owner did not contest this characterization of *Reed* or that a person skilled in the art would have considered *AutoSOCKS* in conjunction with *Reed*. Response at 41-42. Consequently, the Examiner's rejection of claim 14 as obvious should be maintained.

3. Dependent Claim 15

The Examiner correctly found that *AutoSOCKS* in view of *Reed* renders obvious dependent claim 15. Patent Owner responds by presenting a contorted reading of *Reed*, and asserts that "the identifier of *Reed* is not an IP address." Response at 43. This is incorrect. *Reed* explains that onion-routing "is designed to interface with a wide variety of *unmodified* Internet services by means of proxies" and has been implemented in a wide variety of system that use *proxy servers*, such as web browsing and remote logins." (emphasis added) Fratto ¶ 192. In the *Reed* schemes, packets (in one embodiment) are re-routed according to a quasi-random process through onion routers. The identifiers used to route packet traffic in this scheme unquestionably comprise IP addresses. For example, as *Reed* points out, "[t]hat is, communication between two neighboring onion routers is carried over *a socket connection*, and *packets are routed* (perhaps dynamically) through many hops *by the IP protocol*." A person of ordinary skill in the art considering *Reed* in conjunction with *AutoSOCKS* would, of course, focus on the packet implementation of onion-routing as that model would be the one compatible with the TCP/IP based AutoSOCKS systems. Thus, Patent Owner's key assumption in response to the rejection of claim 15 – that "the identifier of *Reed* is not an IP address" – is simply incorrect, and Patent Owner's response, correspondingly, should be disregarded. Patent Owner also concedes that onion routers maintain tables of identifiers (i.e., which are IP addresses in the packet embodiment taught by *Reed*), against which identifiers are compared. Thus, as the Request explains, *Reed* shows onion-routing schemes that compare IP address to tables of IP addresses maintained by intermediary onion-routers (which may be "second

computers") that transport the IP packets. Request at 113 (citing *Reed* at 7 ("When a data cell arrives, the onion router looks up the cell's identifier in its tables and finds the corresponding outbound identifier. The appropriate cryptographic operation is applied and the encrypted payload is formed and sent along the outbound connection.")) Because a person of ordinary skill would have been motivated to incorporate the onion-routing schemes described in *Reed* into the VPN systems taught by *AutoSOCKS*, that person would have found obvious the additional step specified in claim 15, and the Examiner's rejection of this claim was thus proper.

G. Response to Patent Owner's Arguments Regarding the Rejection of Claim 16 Under 35 U.S.C. 103 Based on *Aventail v3.1* in View of *Boden* (Issue 7)

The Examiner correctly found that *Aventail* in view of *Boden* renders obvious dependent claim 16. As explained in the Request, a person of ordinary skill reviewing *Aventail* would recognize the importance of integrating additional network security techniques into its VPN systems. So motivated, that person would have considered the combined teachings of *Aventail* and *Boden*, the latter of which explains that its techniques are useful for solving the "increased likelihood of IP address conflicts inherent in the use of a virtual private network (VPN)." *Boden* at col.2, ll.32-35. *Boden* further explains that its techniques are designed to be implemented with "no, or only minor changes to routing, in each connected domain." *Id.* at col.2, ll.42-45. *Boden* further teaches methods for integrating NAT and IPSec which uses a dynamically changing set of IP addresses within a pool of available IP addresses, and that if an available IP within the pool cannot be found, the connection is not started and an appropriate error messages is generated. *Boden* thus teaches methods for improving security by employing a process in which IP address information in the header of data packets are compared to a dynamically changing pool (a "window") of valid IP addresses, and which rejects data packets having IP addresses that do not fall within the pool (the "moving window"). In response Patent Owner contends only that "IP addresses" in *Boden* "are not compared, but, rather, retrieved based on an ID." Response at 22. Patent Owner's response attempts to read non-existent limitations into the term "compared." As the claims are not so limited, the rejection as imposed was proper and should be maintained.

H. Response to Patent Owner's Arguments Regarding the Rejection of Claim 16 Based on *Aventail v3.01* (or *AutoSOCKS*) in View of *Boden* (Issue 8)

The Patent Owner does not advance any distinct theories or arguments in response to the rejection of claim 16 over *Aventail v3.01* or *AutoSOCKS* in view of *Boden* relative to the rejection based on *Aventail 3.1* in view of *Boden*. Consequently, the Examiner's rejection of claim 16 in

view of these references as obvious was proper and should be maintained.

I. Response to Patent Owner's Arguments Regarding the Rejection of Claim 17 Under 35 U.S.C. 103 Based on *Aventail v3.1* in View of *Weiss* (Issue 10)

The Request explained why *Aventail* in view of *Weiss* would have rendered obvious to a person of ordinary skill a system comprising a "a checkpoint data structure that maintains synchronization of a periodically changing parameter known by the central computer and the client computer to authenticate the client." *See* Request at 117. The Request explained that checkpoint structures recited in claim 17 were well known, and were described, for example, in *Weiss*. The Office properly found that *Aventail* in view of *Weiss* describes a system that renders obvious claim 17. OA at 20-21. In response, Patent Owner asserts that (1) "[t]he non-predictable codes of *Weiss* do not periodically change and (2) "[t]he non-predictable codes of *Weiss* are not known by the computers of *Weiss*." Response at 47-48. Neither point is correct, relevant or persuasive.

a. The Non-Predictable Codes of *Weiss* Periodically Change

Patent Owner does not seriously contest that the techniques described in *Weiss* are an example of a checkpoint structure that maintains a synchronization of a periodically changing parameter known by the central computer and the client computer. Instead, Patent Owner asserts that in *Weiss,* "these non-predictable codes do not change, let alone periodically change." Patent Owner's assertions make no sense. *Weiss* explains that the codes used to authenticate the client are created at each instance of authentication (i.e., at varying times), and each code will be "new" and "unique." *Weiss* teaches that this technique is to be used to improve security by generating variable, non-predictable time-based codes that are synchronized on separate devices. Fratto ¶196. Patent Owner's assertions ultimately are irrelevant to the claims, which impose no particular "periodicity" requirement, and because the tokens in *Weiss* are generated each time there is an authentication event, are thus "periodic."

b. The Non-Predictable Codes of *Weiss* Would be "Known" by the Client and Server Computers

Patent Owner asserts that in *Weiss,* the computers involved "will not know in advance what a particular non-predictable code will be." Response at 48. This argument is irrelevant and incorrect. First, nothing in the claim requires the computers to know or predict what the "periodically changing parameters" will be in the future. Second, Weiss explains that its system employs a technique that permits the client and the server to generate an identical token at any point in time (e.g., when it is necessary "to authenticate the client"). Indeed, this is an inherent

feature of the well-known SecureID token system described in *Weiss*. Moreover, as explained in the Request, a person of ordinary skill in the art would have understood from *Aventail* that its systems are intended to work with a variety of techniques for authenticating users, including the SecureID systems described in *Weiss*. *See* Request at 117-118; Fratto at ¶196. Thus, Examiner's rejection of claim 17 as being obvious over *Aventail v3.1* in view of *Weiss* was proper.

J. Response to Patent Owner's Arguments Regarding the Rejection of Claim 17 Based On *Aventail v3.01* (or *AutoSOCKS*) in View of *Weiss* (Issue 11)

Patent Owner does not advance any distinct arguments responsive to the rejection of claim 17 based on *Aventail v3.01* or *AutoSOCKS* in view of *Weiss* relative to its arguments regarding *Aventail v3.1* in view of *Weiss*. Consequently, the Examiner's rejection of these claims as being obvious over *Aventail v3.01* or *AutoSOCKS* in view of *Weiss* was proper and should be maintained.

K. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1, 2, 4-7, 9, 10, 12, 13, and 18 Under 35 U.S.C. 103 Based on *Wang* (Issue 13)

As explained in the Request, *Wang* describes a variety of approaches to providing access to secure or legacy resources over broadband (hi-speed) networks. Figure 1 of *Wang* shows (i) client computers ("PC clients") at a remote destination, (ii) a pathway across public, and insecure public networks (*i.e.*, the "local loop", "ATM Access Switch/CO", and "Regional Broadband Network"), (iii) a gateway computer (*i.e.*, "PC-based remote access server"), and (iv) a corporate network on which are secure destination computers (*i.e.*, "Corporate Network" and images of PCs on the corporate network). Each of these elements is then described in *Wang*, with guidance provided as to mandatory and optional functionality of each particular element, component or service.

1. Independent Claim 1 Is Anticipated By *Wang*

The Patent Owner alleges that "none of cited portions of *Wang* relating to the LAA architecture mentions an IP address, much less an 'IP address corresponding to a domain name associated with the target computer,' as recited in claim 1." Response at 52. Patent Owner's analysis ignores the explanations in *Wang* that indicate that IP addresses are employed in the LAA scheme for routing IP traffic. *See, e.g., Wang* at Fig. 5 (showing IP protocol being used for communications). Patent Owner also ignores that *Wang* teaches that its various schemes can be integrated, and would not be considered in isolation. *See, e.g.,* Section 10 of *Wang* (describing concept of "architecture coexistence," wherein a LAC and BAS can co-exist) at p. 22. In addition, Patent Owner ignores that *Wang*, at 15, describes a process of domain name resolution as part of the process of routing a request to a desired destination (i.e., "Based on the user-name and domain

information provided in the authentication of the PPP establishment, the LAC determines the destination…"). A person of ordinary skill would immediately recognize that this passage is referring to a DNS resolution step (i.e., converting a domain name of a target into an IP address).

a. *Wang* Discloses the "Generating" Step of Claim 1

The Patent Owner acknowledges that *Wang* discloses the NSP replying to a query from the BAS "with an IP address and other IP configuration information." Response at 52. As an example, *Wang* discloses the DNS server's IP address. The Patent Owner alleges that the IP address disclosed in *Wang* is not "an IP address corresponding to a domain name associated with the target computer." Under the broadest reasonable construction of claim 1, a "target computer" would encompass the DNS server described in *Wang,* as well as cache servers within the network – each is a computer having information related to the target web site. Because the DNS server, the IP address of which is disclosed in *Wang*, is within the scope of the "target computer," as claimed, *Wang* discloses an IP address corresponding to a domain name associated with the target computer. Additionally, a person of ordinary skill in the art would understand that *Wang* discloses an IP address corresponding to a domain name associated with the target computer, as claimed, because *Wang* lists the IP address of the DNS server *merely* as an example. By the use of "*e.g.*," rather than "*i.e.*," one skilled in the art would understand that the NSP would provide IP address of other computers including the server hosting the target web site.

b. *Wang* Discloses the "Determining" Step of Claim 1

Patent Owner asserts that *Wang* does not *explicitly* show a DNS request transmitted in step (1) of *Wang* requests access to a secure web site. The Request explained that *Wang* shows examples for obtaining access to a secure destination, as they show a user supplying credentials to connect to a corporate network, which is generally understood to be a secure destination. The *only* rationale Patent Owner offers in response to refer to ¶ 65 of Dr. Keromytis' declaration, which asserts in a conclusory manner that *Wang* merely discloses that "the LAC or BAS evaluates the domain name to determine the destination NSP so that the LAC can create a tunnel to the proper LNS or the BVAS can send a query to the destination NSP," and "...this does not require that the LAC or BAS determine whether the destination is a secure destination." Dr. Keromytis has mischaracterized this passage of the *Wang* publication. *Wang* describes processes for initiating a network access session that include a step where a user provides a user name along with a fully qualified domain name, as shown on page 15. Moreover, as explained in the Request, the primary

focus of *Wang* is the provision to remote users of access to secure legacy data resources. *See*, *e.g.*, *Wang* at 5 ("This document presents the Core Network architecture for ADSL service *access to legacy data networks*."); id. at 6 ("CPE Architecture – An architecture that defines the access behavior within customer premises network and the interface to the access and the Core Network . . . ."); id. at 9 ("Two approaches are recommended for access to corporate networks."); id. at 12 (*see* Figure 3). *Wang*, thus, teaches providing client computers access to "secure web sites" within the meaning of claim 1.

c. *Wang* Discloses the "Automatically Initiating the VPN" Step

Patent Owner asserts *Wang* does not show automatic establishment of a VPN because it believes *Wang* does not show encryption of network traffic, arguing that based on proposed constructions of claim 1 in concurrent litigation, it would exclude the examples shown in *Wang*. Patent Owner ignores that in reexamination proceedings, claims must be given their broadest reasonable construction. Patent Owner's assertions about the proper construction of claim terms in this proceeding ultimately are irrelevant, as Section 9.5 of *Wang* plainly discloses that its communications employ "encryption, compression and security." *Wang* at 21.

Patent Owner next asserts that the creation of a tunnel by the LAC is inapplicable to the PTA architecture of *Wang*. Response at 54. The Patent Owner's allegations are incorrect for several reasons. First, Patent Owner incorrectly asserts that one skilled in the art would not consider the teachings in different parts of *Wang* together and thereby would not combine elements of the LAA and PTA architectures. *Wang* at 22; FIG. 10. Contrary to Patent Owner's contention, there is nothing in *Wang* that instructs the person skilled in the art to not combine the various elements being described in *Wang*, and in fact *Wang* teaches the concept of "architecture coexistence," wherein a LAC and BAS can co-exist. Second, that a PPP session may be terminated in the BAS instead the LAC does not support Patent Owner's allegation that automatic initiation of a VPN in LAC is inapplicable to the architecture using BAS – that assertion presumes that the claims expressly require entire path between the client and target computers to be encrypted. *Wang* also describes systems meeting the third limitation of claim 1, which recites simply "initiating the VPN between the client computer and the target computer," (emphasis added). Thus, the fact that the PPP session may be terminated in a BAS is irrelevant, as a PPP session initiated between a client and target computer meets the third limitation of claim 1.

Even if one were to read *Wang* as indicating that establishing a tunnel in a LAC is

inapplicable to the architecture using BAS because the PPP session does not tunnel to the NSP but is terminated in a BAS, the architecture using BAS still meets the third limitation of claim 1 read in its broadest reasonable construction, as the claim merely requires "initiating the VPN between the client computer and the target computer," (emphasis added). One skilled in the art would construe a BAS to be within the scope of the "target computer." Therefore, *Wang* discloses the claimed limitation even if the PPP is terminated in a BAS instead of being tunneled all the way to the NSP.

2. Dependent Claim 4 Is Anticipated by *Wang*

Patent Owner asserts that Section 9.2 of *Wang* discloses an authentication step "after, not prior to" the tunnel by the LAC. This is incorrect. *Wang* states that "[t]he LAC may gather authentication information *while determining the proper tunnel*. The LAC should forward this information to the NSP so that user does not need to re-enter the login information." *Wang* at 20. Further, *Wang* explains that a PPP connection exists between the LAC and the CPE "once the option negotiation is complete and the user is identified." *Wang* at 15. Thus, *Wang* teaches, logically, that authentication must precede establishment of the VPN. Patent Owner also contends that Wang does not inherently disclose "returning an error from the DNS request" if the user is not successfully authenticated. But the claims do not restrict the type of responses that may constitute an "error." Under the broadest reasonable reading of this claim term, a response other than successful establishment of the connection could be an "error." The authentication procedures described in *Wang* thus plainly do return an "error" if the client computer fails to authenticate itself. Consequently, the rejection of claim 4 should be maintained.

3. Dependent Claim 5 Is Anticipated by *Wang*

Patent Owner contests the rejection of claim 5 by asserting that the procedures shown in *Wang* do not show that the processes, prior to automatically initiating the VPN between the client and target computers, determine if the client computer is authorized to resolve addresses of non-secure target computers, and if not so authorized, returns an error to the DNS request. *See* Response at 56. As explained in the Request at pages 129-130, *Wang* shows processes where the user must successfully authenticate in order for that client to establish a connection to a remote network or computer. If the user in this model seeks to connect to a secure network, it must ensure that its credentials authorize the connection. In the scenario where the user wishes to access non-secure resources (e.g., a website on the public Internet), the initial authentication of the user's PPP session will be sufficient to authorize that access. In fact, as described on page 15, once the user

successfully authenticates the PPP session, the user's name and fully qualified domain name (e.g., which may be a non-secure target computer) is retained and passed along to facilitate the subsequent authentication of that user. If the destination requires no further authentication, the user gains access to that destination. In that scenario, the requirements of dependent claim 5 are plainly met – based on the domain name that is provided at the authentication step, the computer establishing the PPP connection will determine access rights of the client (e.g., whether the client can navigate to the target destination). Accordingly, *Wang* discloses the additional limitation of claim 5, and the rejection of this claim was proper.

4. Dependent Claim 6 Is Anticipated by *Wang*

The Patent Owner asserts that *Wang* fails to disclose the additional limitations of claim 6 because pages 16 and 21 of *Wang* fail to disclose "hopping between different IP addresses." One skilled in the art would construe "an IP address hopping scheme" to include what is disclosed in pages 16 and 21 of *Wang*. Accordingly, *Wang* anticipates claim 6.

5. Dependent Claims 2, 7, and 9 Are Anticipated by *Wang*

The Patent Owner failed to identify any reason why *Wang* allegedly fails to disclose the additional limitations of claims 2, 7, and 9. For the reasons set forth in the Request, which are incorporated by reference herein, *Wang* anticipates claims 2, 7, and 9.

6. Independent Claim 10 Is Anticipated By *Wang*

Patent Owner asserts that the limitation "a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested," is not disclosed in *Wang* because *Wang* allegedly fails to disclose the LAC returning an IP address. Response at 59. Patent Owner is incorrect because *Wang* explicitly discloses that "the LAC *determines the destination*" based on the user-name and "*domain information*" provided in the authentication phase of the PPP establishment. *Wang* at 15. The primary function of a "DNS server" is to return the IP address associated with the supplied domain name. This is precisely what is shown by *Wang* in the LAC function. *Wang*, as Patent Owner acknowledges, also shows in the BAS embodiment that the NSP responds to a query from the BAS "with an IP address and other IP configuration information *(e.g.*, DNS server's IP address). This demonstrates not only that the BAS is performing the DNS server function as a proxy (i.e., as an intermediary computer), but that the BAS system expressly includes additional DNS servers.

Moreover, the example in *Wang* of providing the IP address of a DNS server is simply an example, and one skilled in the art would understand that the NSP may provide IP address of other computers including the server hosting the target web site, including via the DNS servers to which it is routing requests. *Wang* thus shows this element of claim 10.

Patent Owner also asserts the limitation "wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer" is not disclosed in *Wang* because VPN is a "secured encrypted tunnel" and in the case of the BAS, "instead of being tunneled all the way to the NSP, the PPP sessions are terminated in a Broadband Access Server (BAS)." (Response at 60) Yet, under the broadest reasonable construction of this claim term, there is no requirement that the entire path from the client computer to the target computer carry encrypted traffic. Thus, *Wang* anticipates this element of claim 10. Similarly, Patent Owner asserts *Wang* does not show the limitation that "wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer" because "*Wang* merely discloses that the LAC creates a tunnel to the proper LNS if one does not already exists" and "a tunnel by itself does not provide encryption of traffic." Response at 60. Patent Owner is incorrect at least because *Wang* expressly teaches that "encryption, compression and security" is to be used in the LAA model, which is the architecture using LAC. *Wang* at 21.

Patent Owner also again asserts that the portions of *Wang* regarding the LAA (*i.e.*, the architecture including LAC) and the PTA (*i.e.*, the architecture including BAS) embodiments cannot be considered together. Rather than providing a technical reason why a person skilled in the art would not read these embodiments together, Patent Owner cites the *Net MoneyIN* decision. Patent Owner's reliance on *Net MoneyIN* is misplaced. That decision did not establish a *per se* rule regarding how a prior art disclosure must be read. Instead, it held simply that the particular reference at issue would not have been read as the defendant had proposed. By contrast, *Wang* expressly teaches that distinct network elements it is describing can be combined under the rationale of "architecture coexistence." *Wang* at 22 and FIG. 10.

The Patent Owner also asserts the Request failed to explain which computer in *Wang* is a gatekeeper computer. In reality, the Request explains this at page 131, explaining that *Wang* describes network designs that use "gatekeeper" computers that allocate VPN resources. For example, Figure 3 (page 12) shows a network design having several gateway computers in the network path between the client computer (the "PC client") and the destination computers. These gateway computers include the "LAC" (a L2TP Access Concentrators, see page 14), the "BAS"

(Broadband access Server, see page 16), and the "NSP" (the Network Service Provider, which is a "collective terminology for Internet Service Provider, Corporate network and Locally Hosted Content provider," see page 6). Further, Section 9.7 of *Wang* explicitly discloses "resource allocation and traffic management" for both LAC and BAS. *Wang* at 21.

7. Dependent Claim 12 Is Anticipated by Wang

The Patent Owner failed to identify any reason why *Wang* did not disclose the additional elements of claim 12. For the reasons set forth in the Request, which are incorporated by reference herein, *Wang* discloses the additional limitations in claim 12.

8. Independent Claim 13 Is Anticipated by Wang

Patent Owner contests the rejection of claim 13 as being anticipated by *Wang* on several grounds. First, Patent Owner asserts the Office Action and the Request improperly assume that the processes and systems shown in *Wang* include a "central computer that maintains a plurality of authentication tables each corresponding to one of the client computers," asserting that *Wang* does not necessarily show use of authentication tables. As the Request explains at pages 139-142, the use of authentication tables by a "central computer" is a necessary and thus inherent feature of the systems described in *Wang*. Specifically, *Wang* describes several VPN designs whereby one of a plurality of clients communicates with a VPN Server and, if the client is successfully authenticated, the VPN Server establishes a VPN between the client computer and a secure destination computer. In each example, a "central computer" authenticates the client computers using information that is unique to a user (*e.g.*, username and password) and which is stored on the central computer. For example, in discussing the L2TP Access Aggregation (LAA) design, which uses the principle of tunneling PPP through a regional broadband network (see page 14), *Wang* explains:

> PPP also allows for authentication to be requested during the negotiation. For this application to work, the LAC must be informed of the user's intended NSP. A **user name along with a fully qualified domain name entered during the PPP authentication phase can provide such information**. Once the option negotiation is complete and **the user is identified**, a PPP connection exists between the LAC and the CPE. The next phase is to extend the PPP session from the CPE to the chosen LNS. (emphasis added)

Id. at 15. In this example, the LAC is a "central computer" that communicates with client computers based on authentication performed by a user, which is only possible if authentication tables containing the credentials of the users are maintained by the central computer. Similarly, in the PPP Terminated Aggregation (PTA) network design (pages 16-19), *Wang* explains:

> The BAS extracts the domain string portion of the user-name and sends off a query to **NSP to authenticate and obtain address information** (e.g., DNS server's address). In the case of IP network, the NSP replies with an IP address and other IP configuration information (e.g. DNS server's address). This information is passed along to the user during the NCP phase for configuring IP transport (based on IPCP). The **BAS maps a user identifier** (e.g. port, session identifier, etc.) to the outgoing NSP port.

Id. at 18. *Wang* explains that in this model, CHAP authentication is employed, which necessarily uses information stored on the server computer to compare to credentials presented by a client computer. A third example is the Virtual Path Tunneling Architecture (VPTA) (pages 19-22). In each of these schemes, *Wang* shows individual client computers being authenticated by a "central computer" using unique information stored by that computer associated with a client computer. *Wang* thus shows processes that establish communications between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables corresponding to one of the client computers. Importantly, the claims do not contain language restricting the meaning of "authentication table" to any particular form or content. Patent Owner's assertion that "authentication tables" must of a particular form must be proven to be present in *Wang*, thus can be ignored, as that assertion presumes that such a requirement is present in the claims. Moreover, page 16 of *Wang* explicitly discloses use of "tables" – stating that a "user-NSP mapping in its *routing tables*." Accordingly, *Wang* discloses the additional limitations in claim 13. Patent Owner also asserts that *Wang* does not disclose use of "authentication tables" to authenticate a particular client. Response at 64. Yet, this is precisely what *Wang* teaches. See, for example, page 16 describing use of "user-NSP mapping in its routing tables."

Patent Owner also asserts that *Wang* does not disclose a "central computer." Again, Patent Owner's assertions rest on the incorrect premise that the claims restrict the meaning of "central computer" so as to exclude what is shown in *Wang*. In reality, they do not, particularly when the claims are read with their broadest reasonable construction. In addition, *Wang* describes use of computers that are functioning in the same role as a "central computer" as specified in the claims. Thus, *Wang* (e.g., page 12 and/or FIG. 3) discloses a "central computer" pursuant to claim 13. Accordingly, the rejection of claim 13 was proper and should be maintained.

9. Independent Claim 18 Is Anticipated by *Wang*

The Patent Owner did not contest that *Wang* anticipates claim 18. For the reasons set forth in the Request, the rejection of claim 18 as anticipated by *Wang* should be maintained.

L. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3

and 8 Based on *Wang* in View of *Aventail* and *AutoSOCKS*

The Patent Owner did not assert that *Wang* in view of *Aventail* (or *AutoSOCKS*) renders obvious the additional limitations of claims 3 and 8. For the reasons in the Request, the rejection of claims 3 and 8 based on *Wang* in view of *Aventail* or *AutoSOCKS* should be maintained.

M. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-4, 6-8, 10, 12, 13 and 18 Based on *Beser* in View of *Kent* (Issue 19).

The Request explained that *Beser* describes 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 third party network device on a public network. *See* Request at pages 161 to 164. Patent Owner does not substantively contest the description of how the *Beser* DNS systems and processes function. Response at 67-68. Instead, Patent Owner challenges the combination of the teachings of *Beser* and *Kent*, on a number of specific theories, none of which are persuasive.

1. Independent Claim 1

The Examiner correctly found that *Beser*, in view of *Kent*, would have rendered obvious claim 1 to a person of ordinary skill in the art. Patent Owner disagrees, arguing that: (1) *Beser* cannot be combined with *Kent*; (2) *Beser* and *Kent* do not make obvious initiating a VPN in response to determining that a DNS request is requesting access to a secure target web site; (3) *Beser* in view of *Kent* does not make obvious generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name; and (4) *Beser* in view of *Kent* does not make obvious initiating a VPN in response to determining that a DNS request is requesting access to a secure target web site. Response at 68-71.

a. A Person of Ordinary Skill in the Art Would Combine the Teachings of *Beser* and *Kent*

Patent Owner asserts that *Beser* teaches away from using encryption in IP tunneling applications, arguing that *Beser* "explains that encryption is 'infeasible' and/or 'inappropriate' in VoIP applications." Response at 69. According to Patent Owner, "*Beser's* disclosed system and method for initiating a tunneling association is intended as an alternative to encryption to address the drawbacks that arise form the teachings of *Kent* (*e.g.,* high computing power), not to encourage use of encryption." Request at 69. Patent Owner's analysis of *Beser* is incorrect and incomplete. Critically, *Beser* does not state that using encryption in IP tunneling schemes is "undesirable." Instead, *Beser* consistently and repeatedly states that use of encryption in IP tunneling schemes (of which its system is one) is conventional and ordinarily should be used. *Beser* at col.1, ll.54-56 ("Of

course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security ('IPSec').") In fact, *Beser* specifically refers to *Kent* (the RFC describing the IPSec protocol) to explain how encryption is conventionally incorporated into IP tunneling schemes.

Certainly, *Beser* does indicate that in certain applications (i.e., "VOIP and multimedia"), using encryption in IP tunneling schemes may raise practical concerns. However, this practical concern in certain applications is not an express teaching (as Patent Owner contends) that IPSec or other forms of encryption should not be used in IP tunneling schemes, or that the *Beser* techniques are an alternative to using encryption. Instead, *Beser* states that these practical concerns do not always arise for these two data types, and do not arise at all for data transfer scenarios other than those two types. As *Beser* explains, even in the two high data volume applications noted, encryption should generally be used. *Beser* at col.2, ll.12-14 (indicating that in a particular VOIP system that uses a VPN, "the tunneled IP packets, however, may need to be encrypted before encapsulation in order to hide the source IP address."). *Beser*, thus, teaches that encryption ordinarily should be used in IP tunneling applications, and not, as Patent Owner contends, that it is incompatible with the IP tunneling schemes shown in *Beser*. *Beser* at col.1, ll. 54-66. And, critically, none of the claims are restricted to implementations requiring high data volume applications that were the focus of cautionary statements in *Beser*.

Patent Owner also simply ignores the disclosures in *Beser* showing use of encryption in its systems. Specifically, *Beser* teaches that queries involving the unique identifier [e.g., a domain name] may be encrypted. *Beser* at col.11, ll.22-25 ("The IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12."). *Beser* thus clearly shows use of encryption in various ways to support secure communication links (e.g., use of IPSec-compliant systems, use during establishment of the secure communication link). And as the claims do not expressly restrict how encryption must to be used, Patent Owner's arguments are ultimately irrelevant.

Thus, contrary to Patent Owner's assertions, a person of ordinary skill in the art would not have concluded "that *Beser*'s tunneling technique [was] intended as an alternative to encryption." Response at 69. Instead, that person would have recognized that *Beser* shows systems that use encryption (e.g., when setting up secure communication links), and that encryption (particularly IPSec) ordinarily should be used in IP tunneling applications it is describing, even for high volume data applications such as VOIP and multimedia. Patent Owner's strained reading of *Beser* is implausible and incorrect, and should be disregarded.

b. *Beser*, in View of *Kent*, Makes Obvious Initiating a VPN in Response to Determining that a DNS Request is Requesting Access to a Secure Target Web Site

Patent Owner next asserts that "*Beser* does not disclose that encryption would be initiated in response to the unique identifier described by *Beser*." Response at 70. Patent Owner apparently is relying on the putative absence of the use of encryption in the *Beser* procedures to assert that the secure IP tunnels being described are not VPNs. Patent Owner is incorrect. As explained in the Request, *Beser* describes processes in which a unique identifier (e.g., a domain name) is used to establish an IP tunnel. Request at 164-65 (citing *Beser* at col.10, ll. 37-41, and col.11, ll. 32-36 ("In one exemplary preferred embodiment, the trusted-third-party network device 30 is a … domain name server")). In *Beser*, a trusted-third-party network device (which may comprise a DNS server) will receive and evaluate a connection request (which may comprise a domain name), compare it to a database of entries, and take additional actions to establish the IP tunnel based on the results of that evaluation. *See, e.g.*, *id.* at col.11, ll. 45-59. Under the inherent nature of how a DNS server functions, the domain name is resolved into an IP address. In addition, as *Beser* teaches, if the domain name sent to the trusted-third-party network device specifies a destination that is unknown to the third-party-network device, the device will not route the request further. *Beser* thus shows processes in which a determination is based on the domain name sent in a DNS request, and determines if the request specifies a secure destination (*e.g.,* the second network device). Moreover, *Beser* explains that encryption may be used in examples of this process described in its disclosure, at least to encrypt the initial data transfers involving identification of the IP addresses of the devices involved in the negotiation process. *Beser* at col.11, ll.22-25.

Beser also describes processes that are "automatic" and transparent to the user. For example, *Beser* explains that, in response to a request containing a unique identifier specifying the location of a second network device, the trusted-third-party network device will negotiate with first and second network devices to establish an IP tunnel between the first and second network devices. *Beser* further explains that the "negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26)." *Id.* at col. 12, ll. 6-19. The private network IP addresses are then used in conjunction with the public IP addresses of the first and second network devices to establish the tunnel between the first and second network devices. *See id.* at col.12, ll. 28-37. These steps occur without any interactions or further action from the user that originally made the request. Again, *Beser* does not instruct those of ordinary

skill in the art to avoid using encryption in its systems as Patent Owner asserts. Instead, it states that ordinarily all IP traffic within a VPN IP tunnel will be encrypted utilizing the techniques described in *Kent* (i.e., under the IPSec protocol). *See id.* at col.1, l.54 to col. 2, l. 18. *Beser* also emphasizes the importance of ensuring the secure and private nature of IP tunnels between the first and second network devices, and points out how encryption may be used to achieve this goal. *See, e.g.*, *id.* at col.2, ll.36-40 ("It is therefore desirable to establish a tunneling association that hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network. Hiding the identities may prevent a hacker from intercepting all media flow between the ends."); col.12, ll.13-19 ("In this manner, the identities of the originating 24 and terminating 26 telephony devices are inside the payload fields 84 of the IP 58 packets and may be hidden from hackers on the public network. The negotiation may occur through the trusted-third-party network device 30 to further ensure the anonymity of the telephony devices (24, 26).")

A person of ordinary skill in the art would have consulted *Kent* because it is expressly referenced in *Beser* as describing the conventional IPSec technique that *Beser* says should be used for IP tunneling. *See Beser* at col.1, ll.54-56. *Kent* is the RFC defining the IPSec protocol, and includes specific examples for establishing VPNs via IP tunneling. *See, e.g.*, *Kent* at 8 ("A tunnel mode SA is essentially an SA applied to an IP tunnel.") The IPSec protocol calls for encryption of all IP traffic being sent between nodes of the VPN network – the protocol is designed to automatically encrypt traffic being sent between nodes. A person of ordinary skill in the art would have relied on *Kent* in conjunction with the teachings in *Beser* to incorporate IPsec in IP tunnels established between a first and second network under the procedures described in *Beser*. Accordingly, *Beser* in view of *Kent* would have rendered obvious claim 1 under 35 U.S.C. § 103.

c. *Beser* in View of *Kent* Renders Obvious Generating from the Client Computer a Domain Name Service (DNS) Request That Requests an IP Address Corresponding to a Domain Name

Patent Owner also contests the rejection of claim 1 by asserting the Request does "not establish disclosure of 'generating from the client computer a Domain Name Service (DNS) request that request an IP address corresponding to a domain name associated with the target computer." Response at 71. Specifically, Patent Owner asserts that *Beser* "discloses a request to initiate a VoIP association, not a DNS request that requests an IP address." Response at 71. Patent Owner concedes that a "unique identifier" in *Beser* "may be, in some instances, a domain name," but incorrectly concludes that "merely including a domain name in the request to initiate a

VoIP association does not transform it into a request for an IP address." Response at 71. Again, Patent Owner mischaracterizes the actual teachings of *Beser*. According to *Beser*, the unique identifier specifies the destination (the "target"), and not the trusted third party network device or DNS server. *Beser* further explains that a unique identifier can be a domain name, and that the domain name will be translated into an IP address by the trusted-third-party-network device, which may comprise a DNS server. *See Beser* at col.11, ll.32-36. *Beser* also makes clear that its systems are deployed on the public Internet, and use conventional domain name navigational techniques. *See Beser* at col.2, ll.43-68. Indeed, in its VOIP ("Voice-Over-IP") examples, the *Beser* methods must employ IP addresses of the origination and destination devices that are communicating with each other via a secure IP tunnel. Thus, plainly, *Beser* teaches methods that generate on a client computer DNS requests that request the IP address of the target computer.

d. *Beser* in View of *Kent*, Renders Obvious Determining Whether the DNS Request is Requesting Access to a Secure Web Site

Patent Owner next asserts that *Beser* does not disclose "determining whether the DNS request transmitted in step (1) is requesting access to a secure web site." In particular, Patent Owner asserts that comparing a request against a table of subscribers "simply does not disclose that this list of numbers has any purpose related to security." Response at 72. Patent Owner's contorted logic must be ignored. *Beser* plainly shows that a request made by a client computer is for a target computer, and that the trusted-third-party network device receives and evaluates that request; if the trusted-third-party network device determines the request is for an authorized destination, it then facilitates the establishment of a secure IP tunnel between the requesting entity and that destination. Integral to this process, as *Beser* explains, is the step of determining if the destination is an authorized destination (i.e., is a secure destination). If the destination is unknown, it is not "secure" under the *Beser* model, and the trusted-third-party network device will not attempt to establish secure IP tunnel between that destination and the requesting device.

As it has done in many other places in the Response, Patent Owner presumes that the claims require a particular application, technique or condition. Here, Patent Owner asserts that the destinations shown in *Beser* must be on a list maintained for "security." There is no language in the claims addressing the motivation for designating a destination as secure. More to the point, *Beser* plainly explains that the reason for comparing a request to a pre-defined list of approved destinations is to ensure that secure communications may be established with that destination. As *Beser* explains at col.3, ll.4-9, "The method and system described herein may help ensure that the

addresses of the ends of the tunneling association are hidden on the public network and may increase the security of communication without an increased computational burden." (emphasis added). Consequently, the Examiner's rejection of the claims as being obvious based on *Beser* in view of *Kent* was proper and should be maintained.

2. Dependent Claims 2, 6 and 7 (Issue 19)

Patent Owner presents no distinct basis for contesting the rejection of claims 2, 6 or 7 as being obvious based on *Beser* in view of *Kent* other than those set forth in its response to the rejection of claim 1. The Examiner's rejection of claims 2, 6 and 7 as obvious by *Beser* in view of *Kent* was proper and should therefore be maintained.

3. Dependent Claim 3 (Issue 19)

The Examiner correctly found that *Beser*, in view of *Kent*, would have rendered obvious claim 3. Patent Owner disagrees, asserting the trusted-third-party network device of *Beser* "could not return an IP address of the purported non-secure website because (by virtue of the website being unknown) the trusted-third-party network device would not have an IP address to return. Response at 73. Patent Owner misunderstands the Request and *Beser*. As explained at page 167, *Beser* teaches that the trusted-third-party device may function as a DNS server. A DNS server inherently will resolve and return an IP address. If the request made specifies a non-secure website, the IP address will be simply returned, as this is the inherent function of a DNS server. Request at 167. So, whether or not the target is unknown is irrelevant because the claim specifies only that the trusted-third-party device would not route the request further. Request at 164. Moreover, in *Beser*, websites that are unknown only signifies they are not secure destinations, it does not suggest that their IP addresses cannot be resolved by the DNS server. Accordingly, the Examiner's rejection of claim 3 was proper and should be maintained.

4. Dependent Claim 4 (Issue 19)

The Examiner correctly found that *Beser* in view of *Kent* renders obvious claim 4. In response, Patent Owner asserts that *Beser* does not disclose determining whether a client computer is authorized to establish a VPN. However, for the reasons discussed above, Patent Owner incorrectly describes *Beser, inter alia*, by asserting that "*Beser* does not disclose returning an error in response to a request to initiate a VoIP connection, much less in response to a DNS request." Response at 73-74. This is also incorrect. *Beser* shows that when authentication fails (i.e., when a non-secure destination is requested), the system described in *Beser* will fail to establish an IP tunnel. *Beser* also teaches that authentication can be required of a client seeking to establish a

connection with a destination. *See Beser* at col.11, ll.22-25 ("The IP packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12."). Accordingly, the Examiner's rejection of claim 4 was proper.

5. Dependent Claim 8 (Issue 19)

The Examiner correctly found that *Beser*, in view of *Kent*, renders obvious claim 8. Patent Owner responds that *Beser* does not disclose "determining whether a DNS request is requesting access to a secure web site." Response at 74. But, for the reasons discussed above, this is incorrect. In at least one embodiment, *Beser* shows the trusted-third-party device functioning as a DNS server that would inherently resolve and return an IP address associated with a domain for a non-secure website. Request at 169. Whether or not the DNS request is specifying an authorized destination is irrelevant, as the trusted-third-party device would not route the request further if it specifies an insecure destination. Request at 164. Moreover, that a destination is unknown does not mean their IP address cannot be resolved using the conventional DNS server function. Accordingly, the Examiner's rejection of this claim as rendered obvious by *Beser* in view of *Kent* was also proper and should therefore be maintained.

6. Independent Claim 10 (Issue No. 19)

As explained in the Request, *Beser*, in view of *Kent*, describes a system including a DNS proxy server that establishes a VPN in response to a determination that a DNS request made on a client computer is requesting access to a secure computer, together with a gateway computer that allocates resources for the VPN. *See* Request at 169-73. Consequently, the Office properly found that *Beser*, in view of *Kent*, describes a system that anticipates claim 10. OA at 25-26. In response, Patent Owner asserts that (1) "*Beser* in view of *Kent* does not disclose or suggest a DNS proxy server;" (2) *Beser* in view of *Kent* "does not disclose or suggest returning an IP address for a requested domain name if it is determined that access to a non-secure website has been requested" and (3) *Beser* in view of *Kent* "does not disclose or suggest a request from a client computer to look up an IP address for a domain name. Response at 75-77. Each of these is incorrect.

a. *Beser* in View of *Kent* Discloses a DNS Proxy Server

The Examiner correctly found that *Beser* describes a "DNS Proxy Server" within the meaning of claim 10. *Beser*, in particular, describes the trusted-third-party network device as being a device to which requests are routed to be evaluated, and that the device may be a domain name server. Request at 171-72. Patent Owner does not seriously contest that the trusted-third-party network device is a "DNS Proxy Server" according to claim 10; its criticisms again, simply

assert that the overall system in which this device functions does not involve encryption, and thus cannot be considered to establish a VPN.

b. *Beser* in View of *Kent* Discloses Returning an IP Address for a Requested Domain Name If It is Determined That Access to a Non-secure Website Has Been Requested

The Examiner properly found that *Beser* discloses a DNS Proxy Server that returns an IP address for a requested domain name if it is determined that access to a non-secure website has been requested. Patent Owner responds by asserting, again, that *Beser* does not teach that its systems determine whether the destination specified in a request is a "secure" destination or return IP addresses if the destination is not secure. This is incorrect for the reasons noted above. *Beser* explains the trusted-third-party network device can receive a DNS request, determine if it specifies an authorized destination, and then facilitate establishment of a secure IP tunnel between the originating and destination devices if the latter device is authorized. The inherent function of DNS servers is to return an IP address; if the destination is not known to be authorized (e.g., because it is unknown to the trusted-third-party-network device), the tunnel will not be established; however, because it is a DNS server, it will return an IP address. *Beser* also makes clear the purpose of proceeding through this sequence of steps involving the trusted-third-party network device is to ensure the security of the communications between the originating and destination devices. The Patent Owner's assertions thus, are both incorrect and irrelevant.

c. *Beser* in View of *Kent* Discloses Receiving a Request from a Client Computer to Look Up an IP Address for a Domain Name

Patent Owner asserts that *Beser* does not show that "the client computer requests the IP address for a domain name." This is plainly incorrect based on the express teachings of *Beser*. Specifically, *Beser* teaches that a unique identifier may be a domain name, that the trusted-third-party network device may be a DNS server, and that the device will resolve domain names to obtain public and private IP addresses of the originating and destination devices which are needed to establish a secure IP tunnel between those devices. *See, e.g., Beser* at col.12, l.55 - col.13, l.9. Thus, *Beser* plainly discloses a "receiving a request from a client computer to look up an IP address for a domain name." OA at 25-26.

7. Dependent Claim 12 (Issue No. 19)

Beser describes systems including a gatekeeper computer that determines whether the client computer has sufficient security privileges to create a VPN and, if the client lacks sufficient security privileges, rejects the client computer's request. Request at 173-74. Consequently, the

Office properly found that *Beser*, in view of *Kent*, renders obvious claim 12. OA at 25-26. In response, Patent Owner asserts that the *Beser* systems makes no "determin[ation] whether a client computer has sufficient security privileges to create the VPN." This is incorrect. *Beser* explains that the "IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." *Beser* at col.11, ll.22-25. As is inherent in the disclosed authentication methods, a failed authentication would necessarily result in the failure to establish a VPN. Thus, the authentication methods described in *Beser* necessarily are for the purpose of confirming sufficient "security privileges." Moreover, the claims do not require any particular technique for assessing "security privileges" – that term, thus, can encompass the conventional authentication steps described in *Beser*. Accordingly, the Examiner's finding that *Beser* in view of *Kent* rendered claim 12 obvious was proper.

N. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3, 5, 8, 9, 18 Based on *Beser*, in View of *Kent*, in Further View of *Blum* (Issue 20).

1. Dependent Claim 3 (Issue No. 20)

The Examiner correctly found that *Beser*, in view of *Kent*, in further view of *Blum,* would have rendered claim 3 obvious. Patent Owner responds by asserting that the "DNS proxy server" of *Blum* "does not disclose returning an IP address or determining whether a DNS request is requesting access to a secure target web site, and thus does not add anything to the domain name server discloses by *Beser*." Response at 80. As explained in the Request, *Blum* describes a transparent proxy server that determines if DNS requests require a remote connection, and if not, passes the DNS request for handling by a hosts file or local DNS server. Request at 174. *Blum* expressly teaches that its technique may be integrated into the OS-level TCP/IP support of a computer, and that it returns IP addresses in response to the DNS resolution of a domain name. *See, e.g., Blum* at col.8, l.7 - col.9, l.10. As explained above, *Beser* teaches that domain names may be unique identifiers, that the trusted-third-party network device functions as a DNS server and that it uses the unique identifier to securely negotiate IP tunnels between a first and second secure destination. Accordingly, the Examiner's rejection of claim 3 as being obvious based on *Beser* in view of *Kent*, in further view of *Blum* was proper.

2. Independent Claim 5 (Issue No. 20)

The Examiner correctly found that *Beser*, in view of *Kent*, in further view of *Blum,* would have rendered claim 5 obvious. As explained in the Request, *Blum* describes a transparent DNS proxy service that can be integrated into secure communication systems based on TCP/IP and other

Internet standards. *Blum*, thus, provides an example of a system that can pass through DNS requests specifying non-secure web sites that is compatible with the IP tunneling schemes taught by *Beser*, both alone and in conjunction with *Kent*. In response, Patent Owner again asserts that the responses provided in the *Beser* systems in the case of a request to an unauthorized destination are not "errors." Yet, the claims impose no requirements as to the nature of "errors" to be provided. Moreover, as Patent Owner admits (see Response at 81), errors are returned in VPN deployments using IPSec (taught by *Kent*) such as "ICMP error messages." As noted above, *Beser* expressly identifies IPSec as a technique to be used in IP tunneling systems for VPNs. In addition, *Blum* teaches that errors are provided in a variety of scenarios incidental to DNS queries in its scheme. *See* Request at 174. Thus, the step of returning an error from the DNS request if a VPN is not established is taught and suggested by *Beser*, considered in view of *Kent* and further in view of *Blum*, and the Examiner's rejection of claim 5 was proper and should be maintained.

3. Independent Claim 8 (Issue No. 20)

The Examiner correctly found that *Beser*, in view of *Kent*, in further view of *Blum,* would have rendered claim 8 obvious. Patent Owner responds that *Blum* does not disclose "enabling [] communications based on a determination of whether a DNS request is requesting access to a secure website." Response at 82. *Beser* describes systems that enable communications based on whether a domain name supplied to the trusted-third-party-network device specifies an authorized destination. *Beser* also teaches that its systems are deployed on the Internet, and rely on TCP/IP and other Internet communication protocols. *Blum*, as explained in the Request, describes a transparent DNS proxy system that can be integrated into existing solutions, such as those in *Beser*, without modifying client applications or implementing proxy capabilities in those clients. *See id.* at col. 3, ll.49-58. *Blum* expressly teach that the DNS proxy pass-through requests specifying non-secure destinations. *See, e.g.*, *Blum* at col.6, ll.40-57. Given that *Beser* teaches that domain names may be unique identifiers, that the trusted-third-party network device functions as a DNS server and that it uses the unique identifier to securely negotiate IP tunnels between first and second network devices, a person of ordinary skill would have considered *Blum* to be a relevant additional technique for facilitating the routing of traffic requiring DNS resolution. Accordingly, the Examiner's rejection of claim 8 was proper.

4. Independent Claim 9 (Issue No. 20)

The Examiner correctly found that *Beser*, in view of *Kent*, in further view of *Blum,* would have rendered claim 9 obvious. Patent Owner asserts that because "no single reference that

discloses the step of transmitting a message to the client computer to determine whether the client is authorized to establish the VPN [with the] target computer, the Request concedes that the feature is not disclosed in any of the cited references." Response at 83. The Request made no such admission, and in fact explained that *Beser* expressly teaches that authentication credentials may be demanded by the trusted-third-party-network device. *See* Request at 176. The Request also explained that authentication inherently requires an evaluation of credentials which are transmitted to the server assessing authentication. *Id.* Thus, Patent Owner's assertion that because "there are instances in [*Beser* in] which a server may not demand credentials," the additional step of claim 9 is not suggested by *Beser* or the other references must be rejected. Patent Owner's reliance on concepts of inherency are utterly irrelevant – *Beser* plainly shows scenarios where authentication is required. The rejection of claim 9, thus, was proper and should be maintained.

5. Independent Claim 18 (Issue No. 20)

In response to the rejection of claim 18, Patent Owner provides no distinct arguments from those offered other claims. Because those other rejections were proper, the rejection of claim 18 based on *Beser* in view of *Kent*, in further view of *Blum* should be maintained.

O. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3, 5, 8, 9 and 18 Under 35 U.S.C. §103 Based on *Beser*, in View of *Kent*, and Further in View of *AutoSOCKS* (Issue 21).

In response to the rejection of claims 3, 5, 8 and 9, Patent Owner simply incorporates its response to other rejections. No other rejections, however, were based on the combination of *Beser*, in view of *Kent*, and further in view of *AutoSOCKS*. Patent Owner's failure to provide a specific response addressing the merits of the rejections of these claims demonstrate the rejections were proper, and should be maintained.

P. Response to Patent Owner's Arguments Regarding the Rejection of Claim 11 Based on *Beser* in View of *Kent*, and Further in View of *Reed* (Issue 22).

In response to the rejection of claim 11, Patent Owner provides no distinct arguments from those offered other claims. Because those other rejections were proper, the rejection of claim 11 based on *Beser* in view of *Kent*, in further view of *Blum* should be maintained.

Q. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-10, 12-15 and 18 Under 35 U.S.C. §102(a) Based on *BinGO!* (Issue 23).

1. *BinGO!* Discloses All Limitations of Claim 1.

The Examiner correctly found that *BinGO!* anticipates claim 1. Patent Owner responds by asserting that *BinGO!* (i) does not describe a VPN, (ii) does not determine if a DNS request

specifies a secure destination, and/or (iii) does not show automatic establishment of the VPN. Patent Owner advances each of its flawed theories in response to the showing in the Request of three different examples in *BinGO!* that anticipate the claimed methods. Each assertion is incorrect and is based on fundamental errors made by Patent Owner and its expert about what is taught in *BinGO!* and its patent claims. Consequently, rejections based on *BinGO!* should be maintained.

a. *BinGO!* Discloses a VPN Between Client and Target Computers

BinGO! unquestionably describes establishing a VPN between a client and target computer. For example, at page 226 of *BinGO! UG* ("7.5.1. VPN (Virtual Private Network)"), *BinGO!* explains:

> *BinGO!*! **can set up a VPN using the PPTP** (Point to Point Tunneling Protocol). This offers **secure (encrypted) transmission of data via WAN connections**, e.g. over Internet. It could be used, for example, to provide field service staff with low-cost access to data in the company network via Internet and laptop (dialing in via a local Internet Service Provider).

BinGO! also shows authentication of users and encryption of communications between the client and the secure destination. *See* Request at 185-90. *BinGO!* plainly shows establishing authenticated and encrypted communication links that are referred to as VPNs.

Despite this, Patent Owner asserts that *BinGO!* does not show a VPN "between" client and target computers. First, Patent Owner asserts these VPNs are not encompassed by the claims because the *BinGO!* VPN tunnel does not "fully extend" from the client computer to the target computer. Response at 91-92. Yet, the claims do not impose such a requirement, but instead simply specify that a VPN is established "**between** the client and the target computer." Patent Owner's theory also is refuted by its own disclosure. For example, at col.36, ll.25-29, the '135 patent explains "[a]s shown in FIG. 24, a first computer 2401 communicates with a second computer 2402 **through two routers** 2403 and 2404. **Each router is coupled to the other router through three transmission links**. As described above, **these may be physically diverse links or logical links (including virtual private networks)**." (emphasis added). Thus, according to its own disclosure, claim 1 encompasses the precise scenario shown in *BinGO!* where the client and target computer communicate securely with each other through a VPN established between edge routers (such as the BinGO! router). Moreover, *BinGO!* does show computer-to-computer, and computer-to-network connections being established, not simply network-to-network examples.

See, e.g., BinGO! EFR at 82. In fact, examples throughout *BinGO!* show the BinGO! router connecting directly to a secure corporate network rather than via an ISP. *See, e.g., BinGO!* at 53 (Figure 3-7 "Connecting Bingo! to a Corporate Network"). Patent Owner's next assertion is even more illogical – that the claims exclude a scenario where a client computer establishes scenarios where the VPN is established over the Internet to a target computer. *See, e.g.*, Response at 95 (asserting claims exclude scenario where the "VPN under either the PPTP Client-to-VPN Server scenario or the LAN-to-LAN VPN scenario … connect[s to the target computer] to or over the Internet, and not to the corporate network at which the BossPC is located.")

Patent Owner's flawed theories appear to rest on fundamental errors made by its expert, Dr. Keromytis, in portraying the teachings in *BinGO!*. For example, Dr. Keromytis asserts "nowhere in the entire chapter of *BinGO! EFR* describing virtual private networking does *BinGO! EFR* mention that the described alleged VPN services are available for the BinGO! router." Response at 93; Keromytis Dec. at 28-29. In reality, both *BinGO! UG* and *BinGO! EFR* documents repeatedly refer to each other in explaining how to implement various types of VPNs using a BinGO! router. For example, *BinGO! UG* expressly refers to *BinGO! EFR* for details in setting up a VPN using a BinGO! router. *BinGO! UG* at 226, 266; *see also BinGO! UG* at 112. Similarly, the second page of *BinGO! EFR* explains that "[t]his manual provides a complete description of all the complex, separately licensable features available for the BinTEC BIANCA/BRICK and BinGO! routers." *BinGO! EF* at "NOTE" (emphasis added); *see also BinGO! EF* at 2.

Similarly, Patent Owner and its expert present a strained and illogical discussion of connections from a "home office" to a secure corporate network, suggesting that *BinGO!* does not teach or suggest scenarios where a client computer is accessing secure websites or other resources on the secure network. Response at 98; Keromytis Dec. at 32-33. This is simply incorrect – *BinGO!* plainly shows a remote client accessing over a public network secure resources on a corporate network. *See, e.g.*, *BinGO!* at 53 (Figs. 3-7). Similarly, Patent Owner incorrectly asserts that *BinGO!* does not show a remote user accessing files on a corporate network, asserting it only shows accessing files from a local network. *Id.* Yet, *BinGO!* expressly describes scenarios where a client accesses data present on a (secure) corporate LAN from the client computer, which is on a different LAN. *BinGO!* at 17; *see also*, *e.g.*, *id.* at 33 ("If necessary, establish a connection with a remote network (LAN-LAN connection, e.g. to your head office), and **access corporate data from the comfort of your home office**.)). The characterizations of *BinGO!* by Patent Owner and its expert are incorrect and should be ignored. As explained in the Request, *BinGO!* shows client

computers communicating via VPNs with secure target computers.

b. *BinGO!* Discloses the "Determining" Step of Claim 1

Patent Owner next asserts that *BinGO!* does not disclose "determining whether the DNS request transmitted in step (1) is requesting access to a secure web site." Response at 95-96. Again, Patent Owner's assertions conflict with the explicit teachings in *BinGO!*. First, *BinGO!* shows systems that evaluate connection requests and route them based on the content of that request (i.e., whether it specifies that address of a secure destination (e.g., the corporate network) or a non-secure destination (e.g., a public website)). Request at 191-198. *BinGO!* explains this is done by comparing the address specified in the request to information in tables or lists -- If the address in the request matches one of the secure destinations, the BinGO! router automatically establishes the VPN with the secure destination. *Id.* at 191-92 (explaining discussions in *BinGO!* of use of local host files and/or router-based tables storing routing information to evaluate and act on requests to secure or non-secure destinations). *BinGO!* also shows that the BinGO! router can be configured to pass DNS requests specifying non-secure destinations to a local network or public DNS server, or to a DNS server maintained by the corporate network. *Id.* In each example, the destination in the request determines whether a VPN will be established with the destination.

BinGO! EFR provides further examples of Bingo! routers configured to establish VPNs based on the destination specified in a connection request (e.g., describing process where secure target selected by checking a VPN menu list and setting up VPN based on that determination). *See BinGO! EFR* 73-81. *BinGO!* also describes other uses of information in a connection request to establish a VPN. For example, *BinGO!* discloses that the BinGO! router may "verify the VPN partner by the IP address the VPN partner can be reached at on the Internet." *See BinGO! EFR* at 76. Thus, contrary to Patent Owner's assertions, *BinGO!* shows the target destination address is used to determine whether that request is routed to a secure destination or a non-secure destination.

c. *BinGO!* Describes Automatic VPN Establishment

Patent Owner admits that *BinGO!* automatically establishes a VPN. Response at 101 ("Even if **the alleged VPN between the user's PC and the BossPC is automatically initiated in response to an event**, the alleged VPN between the user's PC and the BossPC is nevertheless automatically initiated in response to the alleged DNS request or any determination that the alleged DNS request is requesting access to a destination.") The only issue the Patent Owner disputes is that *BinGO!* shows that the "event" that triggers this automatic VPN establishment can be a DNS

request. Patent Owner's evasive and contorted discussion of this issue, like its other assertions about *BinGO!*, is simply wrong.

BinGO! clearly shows **requests specifying secure destinations** (e.g., a DNS request specifying "BossPC" on the corporate network) **trigger** the **automatic establishment** of authenticated and encrypted communications between the client and target computer. *See, e.g., BinGO!* at 41 ("You only need network addresses and netmasks of the WAN partner (head office) if, in addition to a LAN-LAN connection, you are configuring for Internet access. If you are not configuring for Internet access, BinGO! will be configured so that all data not destined for your own local network will be **automatically forwarded to the WAN partner** (default route).") In particular, as explained at 191-198 of the Request, when a user specifies a destination on the secure corporate network (e.g., BossPC), the content of that request is evaluated. If the destination is an IP address known to be on the secure corporate network, the BinGO! router will initiate a connection with the gateway to the corporate network, authenticate the user, and ordinarily will encrypt/decrypt the network traffic sent and received from that remote destination. *See, e.g.,* Request at 186-188 (discussing encryption/ VPN handling in *BinGO! UG* and *BinGO! EFR*); *id.* at 191-196 (discussing *BinGO!* descriptions for routing of traffic to "partner's network" based on DNS request). In one example, *BinGO!* explains that the BinGO! router can be set up to either route the traffic from that client computer to the specified corporate network or to pass it through to a local ISP, depending on what destination is specified in the request. In fact, it is fundamental in these examples in *BinGO!* that the address of the destination determines the actions the BinGO! router will take. It is also immaterial that the BinGO! router can be configured to route all traffic (in one embodiment) to the corporate network for evaluation of the DNS request – *BinGO!* plainly shows other embodiments where the request is evaluated on the local network on which the client computer resides, or even on the client computer itself. *BinGO!* also explains that DNS resolution is part of its design – domain names can be resolved by a local DNS server on the client network, data on the client computer, by an ISP or by a DNS server on the corporate network. Patent Owner further mischaracterizes *BinGO!* by asserting that it states that a DNS server is "unable to translate computer names, and such a connection to the provider would be a waste of time, not to mention money." Response at 100. *BinGO!* is actually explaining that one "set[s] up your own Domain Name Server in which all the names of the PCs in your partner's network and their corresponding IP addresses that you want to reach are listed." *BinGO! UG* at page 88. *BinGO!* also explains that a user can "save the IP address to name arrangements on your PC." *Id.* Either of these options will

translate the name of a computer that is the destination of the request into an IP address. *BinGO! UG* at 87-88.

Moreover, *BinGO!* also indicates that the BinGO! router can be configured to use the "the IP address the VPN partner can be reached at on the Internet" (which is obtained from the DNS request) to verify the destination and establish the VPN. *BinGO! EFR* at 76. This is another example of *BinGO!* showing use of the destination specified in the connection request to establish the VPN. This example also illustrates that connections may be designed to establish secure pathways between individual computers, rather than simply between networks. *BinGO! EFR* at 82 (showing secure computers on VPN server communicating directly with VPN client computer). In view of these observations, and as explained in the Request, *BinGO!* shows all of the elements of claim 1. Consequently, the rejection of claim 1 should be maintained.

2. *BinGO!* Discloses All Limitations of Dependent Claims 2-10 and 12.

The Examiner correctly found that *BinGO!* anticipates claim 2-10 and 12. In response, Patent Owner present a series of mischaracterizations or irrelevant observations about the teachings of *BinGO!*. These should be disregarded and the rejections maintained.

Claim 2: Patent Owner asserts *BinGO!* shows that a user may query a local file ("LMHOSTS file") to resolve a DNS request, and that this means that steps (2) and (3) of claim 2 would be performed at the client computer. This observation ignores that other embodiments described in *BinGO!* that show a separate DNS server that resolves the DNS request. In those configurations, the determination of whether a DNS request is specifying a secure web site is made on computer other than the client computer. *See* Request at 198-99.

Claim 3: Patent Owner asserts that *BinGO!* does not show that requests for non-secure websites are resolved and returned to the client computer. Yet, this is shown to be an integral feature of the BinGO router. As *BinGO!* explains, in a typical configuration, a request that does not specify a destination on the corporate network is passed to a DNS on the local network or an ISP for resolution. Request at 199-200; *see also BinGO! UG* at 91-92 (As soon as you enter www.bintec.de, for example, in the browser, the PC sends a DNS request to BinGO! – as BinGO! is known as a DNS proxy server. BinGO! can not translate the name itself and sends the packet with the DNS request along the default route to the provider. There the name www.bintec.de can be resolved. The DNS request is successful and in reply the PC receives the IP address for the name www.bintec.de.")

Claim 4: Patent Owner asserts *BinGO!* does not show a process of determining that a user

is authorized to resolve addresses not located at the network before establishing a VPN. Response at 109-11. This is incorrect – *BinGO!* shows that a user cannot access the *BinGO!* router (and cannot establish a VPN) until that user is authorized via password, and that if the user is not authorized, *BinGO!* will return an error. Request at 200-01; *BinGO! UG* at 243. *BinGO!* also shows a process for authenticating a specific DNS request. Specifically, *BinGO!* states that "[b]oth the ISP and the VPN Server will typically want to verify the initiating partner during connection establishment. Authentication is performed inband using PAP, CHAP, or MS-CHAP." *See BinGO!* at 84. This VPN authentication process similarly authorizes the establishment of a VPN with a target computer. Accordingly, claim 4 is anticipated by *BinGO!*.

Claim 5: Patent Owner asserts that *BinGO!* does not show that the client computer must be authorized to resolve addresses of non-secure target computers or that an error will be returned if the user is not authenticated. Response at 110-12. Yet, in at least one embodiment, *BinGO!* shows BinGO! routers will require authentication of a user before access to the router is permitted, whether the request is specifying a secure or non-secure destination. A failed authentication will return an error to the user in these embodiments. *BinGO!* also shows that client computers may be authorized or not authorized to access public destinations outside the corporate network. *See, e.g., BinGO! UG* at 90-91; Request at 201-02. Thus, *BinGO!* anticipates claim 5.

Claim 6: Patent Owner asserts that the Network Address Translation (NAT) and OSPF protocols do not describe those features of the claim. Response at 114-15. However, Patent Owner falsely reads this disclosure without applying the understanding of one of ordinary skill in the art at the time of the invention. For instance, OSPF protocol was an adaptive routing protocol that creates an IP address hopping scheme for communications between client and target computers. Accordingly, the limitations of claim 6 are disclosed by *BinGO!*.

Claim 7: Patent Owner asserts that *BinGO!* does not disclose use of "IP hopping" schemes. As the Request explained, at least two examples of IP hopping schemes (NAT and OPSF) are shown as being integrated as options in *BinGO!*. *See, e.g.,* Request at 202-03. Patent Owner's assertions presume that claim 7 expressly limits the nature of IP hopping schemes at issue; it plainly does not. Consequently, Patent Owner's assertions must be disregarded.

Claim 8: As shown in the request, in three different configurations, a DNS proxy server, which can be the BinGO! router, will determine how to route and handle a request based on the destination specified in the request. *See* Request at 204-05. In response, Patent Owner simply reiterates that *BinGO!* nowhere shows a "determination" step being made. *See* Response at 117-

18. As explained above, this is simply incorrect.

Claim 9: Several examples in *BinGO!* were identified in the Request of "messages" being sent to and from the client computer as part of the authentication processes for that client. *See* Request at 205. Patent Owner asserts that none of these examples show a message is transmitted to a client computer to determine if that computer is authorized to establish a VPN. Response at 118-19. For example, Patent Owner asserts that one of these examples merely describes access to configuration of the BinGO! router. Patent Owner is again incorrect. The examples identified in the Request show authentication steps that must be successful before the client computer can use the BinGO! router to access secure or non-secure destinations. *See id*. Patent Owner also ignores the separate authentication of a VPN request. *See BinGO! UG* at 84

Claim 10: Claim 10 requires many limitations similar to claim 1, and further requires "a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server." A BinGO! router is a gatekeeper as it is separate from the client computer and allocates resources for the VPN between the client computer and the secure web computer in response to the DNS request. *BinGO! UG* at 15, 17, 61, 84-85, 87-88, and 140. In response, Patent Owner simply asserts *BinGO!* does not establish a VPN "in response to the request by the DNS proxy server." *See* Response at 119-22. As explained above, this is simply incorrect.

Claim 12: As noted above, *BinGO!* shows several examples where a client computer must be successfully authenticated to use a BinGO! router to access secure or non-secure destinations. In response, Patent Owner simply repeats its arguments that *BinGO!* does not show establishment of a VPN. Response at 122-23. As this is incorrect, the rejection should be maintained.

3. *BinGO!* Discloses All Limitations of Claim 13

The Examiner correctly found that *BinGO!* anticipates claim 13. Patent Owner responds by asserting that *BinGO!* does not disclose the step of "authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client," Response at 126-27. Patent Owner asserts that the elements shown in *BinGO!* are not "arranged as in the claim." Response at 125. Patent Owner is incorrect, both as to its assumption the claims require a particular order, and in its characterizations of *BinGO!*. As to the latter point, *BinGO!* discloses the claimed authentication tables by virtue of its use of protocols as PAP, CHAP, and MS-CHAP. *See, e.g., BinGO! EFR* at 84 ("Both the ISP and the VPN Server will typically want to

verify the initiating partner during connection establishment. Authentication is performed inband using PAP, CHAP, or MS-CHAP.") A person skilled in the art would have known these authentication protocols store user/password combinations in the form of an authentication table, and that such tables are used to authenticate a request from a particular client. Patent Owner simply ignores this disclosure in *BinGO!*. Also, *BinGO!* discloses a VPN menu that specifies which PPP Authentication Protocol to use for any given partner. *See BinGO! EFR* at 76. *BinGO!* thus discloses "authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client."

Patent Owner also asserts that *BinGO!* does not disclose the step of "responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer." Response at 129. Again, Patent Owner ignores *BinGO!*'s authentication procedure, described on page 84, which explains that when a user requests establishing of a virtual private link, authentication is required. *See BinGO! EFR* at 84. Absent authentication, the BinGO! router will not allocate resources to establish the virtual private link. *See id.* Accordingly, *BinGO!* clearly discloses that the allocation of resources in response to a determination that the request is from an authorized client, as required by claim 13. Thus, as *BinGO!* discloses each limitation of claim 13, the rejection should be maintained.

4. *BinGO!* Discloses All Limitations of Dependent Claims 14, 15 and 18

Claim 14: Patent Owner asserts that *BinGO!* does not disclose that the internal host address is periodically changed, let alone periodically changed according to a known sequence. Response at 133. However, Patent Owner's reading of *BinGO!* rests on its incorrect understanding of what *BinGO!* would have taught a person of ordinary skill by its disclosure of use of a variety of Network Address Translation (NAT) schemes. *BinGO! UG* at 244-249. NAT schemes inherently function by changing at least one field in a series of data packets periodically according to a known sequence. As the Request explains, citing RFC 2663, NAT devices provide a transparent routing solution by modifying end node addresses en-route and maintaining state for these updates so that datagrams pertaining to a session are routed to the right end-node in either realm. Request at 212. Thus, *BinGO*! describes the limitations of claim 14.

Claim 15: Patent Owner identifies no technical deficiency with the explanation of how *BinGO!* anticipates claim 15, asserting only that the elements shown in *BinGO!* are not "arranged as in the claim." Response at 134. This response simply ignores the contents of *BinGO!*, which

clearly explains that NAT implemented on a BinGO! router functioned by taking an outgoing IP packet, and changing the IP address in the packet to a predefined address corresponding to the BinGO! router's IP address or that of another network device. *BinGO! UG* at 249 (explaining that BinGO! router may be configured to use the IP address of a host on the LAN, and that if no other address is specified, then "*BinGO!*! is assumed as the destination.") (emphasis added). Thus, *BinGO!* discloses all the limitations of claim 15.

Claim 18: In response to the rejection of claim 18, Patent Owner provides no distinct arguments relative to those offered for responding to rejections of other claims. Because those other rejections were proper, the rejection of claim 18 based on *BinGO!* should be maintained.

R. Response to Patent Owner's Arguments Regarding the Rejection of Claim 11 Under 35 U.S.C. §103 Based on *BinGO!* in View of *Reed* (Issue No. 24)

The Examiner correctly found that claim 11 would have been obvious based on *BinGO!* in view of *Reed*. Patent Owner incorrectly asserts that the intended purpose of *BinGO!* is to directly dial into a destination and that the onion routing scheme renders *BinGO!* unsatisfactory for its intended purpose. Response at 136. Contrary to Patent Owner's assertions, *BinGO!* never suggests that a direct dial is the sole "intended purpose" of its communication schemes, or that any other method for transporting packets would be "unsatisfactory." As Patent Owner provides no other distinct arguments from those offered other claims and those other rejections were proper, the rejection of claim 11 based on *BinGO!* in view of *Reed* should be maintained.

S. Response to Patent Owner's Arguments Regarding the Rejection of Claim 16 Under 35 U.S.C. §103 Based on *BinGO!* in View of *Boden* (Issue No. 25)

In response to the rejection of claim 16, Patent Owner provides no distinct arguments from those offered other claims. Because those other rejections were proper, the rejection of claim 17 based on *BinGO!* in view of *Boden* should be maintained.

T. Response to Patent Owner's Arguments Regarding the Rejection of Claim 17 Under 35 U.S.C. §103 Based on *BinGO!* in View of *Weiss* (Issue No. 26)

In response to the rejection of claim 17, Patent Owner provides no distinct arguments from those offered other claims. Because those other rejections were proper, the rejection of claim 17 based on *BinGO!* in view of *Weiss* should be maintained.

U. There are No Secondary Considerations Linked to the Claims

Patent Owner provides alleged secondary considerations that are little more than unsupported statements by its own Chief Technology Officer, Robert Short. First, Patent Owner

contends that there was "long felt need for a system that could establish a VPN communication link in a simple and straightforward manner, because 'a solution that was difficult for an end-user to employ would likely have led to lack of use or incorrect use." Response at 139. Similarly, Patent Owner contends there was a "general understanding that reliable security could only be achieved through difficult-to-provision VPNs." Response at 140. However, Patent Owner has not demonstrated that the claimed invention, rather than the prior art DNS systems taught in the prior art (e.g., *Aventail, Wang, Beser, BinGO!, Kent* or combinations thereof) are responsible for addressing these long-felt needs. Similarly, the Patent Owner contends there is evidence of significant commercial success. Again, however, Patent Owner provides no evidence that whatever commercial success the company has experienced—which is apparently solely limited to licensing revenue based on products and services marketed by other parties—is attributable to the features of the claimed invention. Consequently, Patent Owner's putative evidence of secondary considerations is irrelevant to the rejections for obviousness imposed by the Examiner and those rejections should be accordingly maintained.

For all of the reasons set forth above, the Third Party Requester contends that the Patent Owner has not rebutted the Examiner's rejection of the claims on any of Issues 1-26 of Office Action of February 15, 2012. The rejection of all the claims under each of those Issues should, accordingly, be maintained. Requester hereby incorporates and reiterates the reasons set forth in the Request as to why each of claims 1 to 18 is unpatentable over the references and upon the grounds set forth in the Request.

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: October 4, 2012