cannot find, anywhere in the '504 specification where the Patent Owner refers to the secure domain name service 3313, alone and by itself, as a *system*.

Accordingly, the Patent Owner's argument that the "system" of claim 1 must reside in a single server is an improper attempt to introduce a new limitation, e.g., "wherein the domain name server system is embodied in a single server that does not depend on any assistance from another server in performing its operations." *All* of the Patent Owner's remarks regarding the rejection of claim 1 based on Aziz are premised on this improper rewriting of the claim. (Response at 29.) As such, the Patent Owner's arguments are fatally flawed from the outset, and the Examiner's rejection remains proper and supported by Aziz. Nonetheless, Requester provides a detailed response to each argument below.

(i) Aziz's SX Records Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Patent Owner argues, on pages 29-30, that the "SX record includes the name or address of firewall 110, which is separate from the alleged domain name service system, NS 120." (Response at 29-30.) This argument fails for several reasons.

First, as noted above, the Patent Owner is improperly attempting to rewrite claim 1 to recite a "domain name service ~~system~~ server" through attorney argument. The Patent Owner's assertion that only outside NS 120 can be part of the claimed "system" is without merit. Accordingly, the SX records for other components of the Aziz system, such as for firewall 110 used to establish a secure communication link with inside name server 130, are an "indication that the domain name service system supports establishing a secure communication link" as recited in the claim.

Second, Aziz discloses that the outside NS 120 includes an SX record for itself: "Tasks that the network administrator performs to configure outside NS 120 include defining an SX resource record type and adding appropriate records to the name server database for outside NS 120." (Aziz, 8:66-9:2.) Thus, even under the Patent Owner's improper interpretation of the claim, Aziz teaches all of the limitations of claim 1.

The Patent Owner then continues by comparing Aziz's disclosure to the admitted prior art in the '504 patent specification. Absent from this comparison, however, is analysis comparing Aziz's disclosure to the claim limitation at issue. Aziz teaches not only name resolution capabilities, but also an indication of support for establishing a secure communication

link (e.g., storing and providing the addresses of secure exchangers). Patent Owner's analysis of the two prior art systems—without addressing the Aziz's teaching of an "indication"—is not relevant.

The Examiner's rejection of claim 1 as anticipated by Aziz is proper and should be made final.

(ii) Aziz's KEY and SIG records Disclose an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Patent Owner argues, at pages 31-32, that the "KEY or SIG resource records in *Aziz* include no indication about the capabilities of *the alleged domain name service system itself*," (Response at 31) which the Patent Owner argues must be the outside NS 120 and nothing more. This argument fails for several reasons.

First, as noted above, the Patent Owner is improperly attempting to rewrite claim 1 to recite a "domain name service ~~system~~ server" through attorney argument. The Patent Owner's assertion that only outside NS 120 can be part of the claimed "system" is without merit.

Second, the KEY and SIG records are stored on and provided by the outside NS 120. (Aziz, 9:34-38.) The KEY and SIG records support the establishment of a secure communication link, for example, by "verifying signed records upon receipt." (Aziz, 9:38-40.) Thus, their presence on the outside NS 120 is an "indication that the domain name service system supports establishing a secure communication link." Providing the KEY and SIG records upon request, as the outside NS 120 does, is similarly an "indication."

Finally, Aziz discloses that the outside NS 120 includes an SX record for itself: "Tasks ... to configure outside NS 120 include defining an SX resource record type and adding appropriate records to the name server database ***for outside NS 120***." (Aziz, 8:66-9:2 (emphasis added).) Even under the Patent Owner's improper interpretation of the claim, Aziz teaches all of the limitations of claim 1.

(iii) Aziz's "Information Used for Secure Communications with Protected Hosts" Discloses an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Patent Owner argues, at pages 32-33, that Aziz's SX record is a "conventional feature of a domain name service system that the '504 patent recognizes and distinguishes." (Response at 32.) This argument fails for several reasons.

The Patent Owner provides no citation—and Requester can find none—where the '504 Patent "recognizes and distinguishes" the SX records taught by Aziz. More importantly, the Patent Owner does not identify how the language of the claim distinguishes Aziz's SX records. As such, the Patent Owner makes only a "general allegation that the claims define a patentable invention, without specifically pointing out how the language of the claims patentably distinguishes them over the references." (MPEP § 2666.)

The Patent Owner also argues that the SX record is used "'on a client,' which is separate from the alleged domain name service system, NS 120." (Response at 32.) As noted above, the Patent Owner is improperly attempting to rewrite claim 1 to recite a "domain name service ~~system~~ server" through attorney argument. The Patent Owner's assertion that the claimed "system" must be found in a single server is unfounded. As previously noted, the '504 specification repeatedly uses the word "system" to refer to a collection of multiple components. The client-side resolver, which communicates with the NS 120 to obtain and use domain name information, is therefore properly considered a part of the claimed "domain name service system."

The Examiner's rejection is proper and should be made final.

(iv) Aziz's Reference to RFC 2065 Discloses an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link"

The Patent Owner argues, virtually without explanation, that a bit in a KEY resource record cannot be an "indication that the domain name service system supports establishing a secure communication link." This argument fails because it is directly contradicted by the teachings of RFC 2065.

Aziz teaches that the bit in question—"an assertion that the host speaks IPSEC" (RFC 2065 at 12)—is stored in a KEY resource on the domain name server. The domain name server sends the KEY resource to a requester to indicate to the requester whether the host can establish a secure communication link. Thus, the domain name server supports the establishment of a secure communication link and includes an indication thereof.

The Patent Owner's argument that Aziz lacks an indication of support for establishing a secure communication link is both unexplained and inexplicable. The Examiner's rejection is proper and should be made final.

b. Independent Claims 36 & 60

Regarding independent claims 36 and 60, the Patent Owner's relies on the same improper and erroneous arguments related to claim 1 that are conclusively refuted above. Accordingly, the rejections of claims 36 and 60 should be reaffirmed and made final.

c. Dependent Claims 5, 23, & 47

The Examiner properly rejected claims 5, 23, and 47 because Aziz teaches:

- A "'signature,' resource record can be used to authenticate the data in other resource records." (Aziz, 5:67-6:1.)
- "Authenication [*sic*] means that the host is assured that the message is from the client that the message claims." (Aziz, 3:22-24.)
- "[C]ryptographic methods (or equivalent security techniques) are commonly used to ensure various aspects of privacy, integrity, and authentication." (Aziz, 3:27-29.)

Additionally, Aziz refers to RFC 2065 for the well-known details of the secure domain name service (See Aziz, 6:11-21), and RFC 2065 states that "***Requests can also be authenticated*** by including a special SIG RR at the end of the request." (RFC 2065 at 9 (emphasis added).)

Accordingly, Aziz discloses that (i) messages from clients—e.g., requests—can be authenticated to verify that the message correctly identified the client that sent the message, and (ii) this authentication process is accomplished using cryptographic methods. Accordingly, Aziz teaches "to authenticate the query using a cryptographic technique" as recited in claims 5 and 23, and the similar limitation in claim 47.

The Patent Owner argues at page 35 that "merely disclosing that the SIG resource record '*can be used* to authenticate data' does not disclose that "*the domain name service system* is configured to authenticate' anything." This argument fails because it does not take into account the full teachings of Aziz's secure domain name service. Aziz's system operates using the secure DNS technology "well known to those of skill in the art" (Aziz, 6:13) in which "***Requests can also be authenticated*** by including a special SIG RR at the end of the request." (RFC 2065 at 9 (emphasis added).) The Patent Owner's argument is without merit.

d. Dependent Claim 8

The Examiner properly rejected claim 8 because Aziz teaches:

- Segregating a portion of network as a "protected zone." (Aziz, 5:11-18.)

- Providing an authorized client outside the protected zone to access to machines within the protected zone using encrypted communications. (Aziz 9:5-9.)
- Connecting an "outside" name server to the network outside of the protected zone, and connecting a second "inside" name server within the protected zone. (Aziz, 5:11-18.)

Accordingly, Aziz teaches (i) creating a virtual private network including secure communication links between machines within a protected zone and authorized clients outside the protected zone; and (ii) connecting secure domain name servers both within and outside the protected zone. Thus, Aziz teaches that "domain name service system is connectable to a virtual private network through the communication network."

The Patent Owner argues that "outside NS 120, and not inside NS 130 of Aziz, is the alleged domain name service system." (Response at 35.) This argument depends on the Patent Owner's improper attempt to rewrite claim 1 to recite a "domain name service ~~system~~ server" through attorney argument. (See discussion above.) The Patent Owner's assertion that *only* outside NS 120 can be part of the claimed "system" is without merit. At a minimum, all of Aziz's name servers, including outside NS 120 and inside NS 130, are properly considered part of Aziz's "domain name service system."

The Examiner's rejection is proper and should be made final.

e. Dependent Claims 17 and 41

The Patent Owner does not raise any argument specific to the limitations of claims 17 and 41, relying solely on its failed reasoning with respect to parent claims 1 and 36. Accordingly, the rejection of claims 17 and 41 is proper and should be made final.

f. Dependent Claims 18 and 42

The Examiner properly rejected claims 18 and 42 because Aziz discloses:

- Organizing domain names "into smaller segments, which are referred to as 'zones' (e.g., eng.sun.com and corp.sun.com)." (Aziz, 1:58-60.)
- Each zone "has its own database (the 'zone database') containing the names, addresses, and other information for the machines in that zone." (Aziz, 1:66-68.)
- Access to a zone can be restricted such that computers within the zone are not publicly visible, in which case the zone is a "protected zone." (Aziz, 2:20-22.)
- It is desirable to permit "authorized clients outside the protected zone to communicate

with hosts inside the protected zone." (Aziz, 2:53-54.) To achieve this, a firewall is configured to handle "encrypted communications between authorized client 210 and machines inside protected zone 180." (Aziz, 9:5-7.)

Accordingly, Aziz teaches that (i) a domain name can be divided into segments, (ii) a domain name segment can refer to computers within a protect zone, (iii) the computers within the protected zone are reachable, from outside the zone, through secure communication links. Thus, Aziz teaches that a domain name "is reserved for secure communication links" as recited in claim 18 and the similar limitation in claim 42.

The Patent Owner agrees that Aziz teaches associating a domain name with a protected zone, hiding machines within the protected zone from public view, and allowing secure communications with the machines in the protected zone. (*See* Response at 37.) Without explanation, however, the Patent Owner asserts that these teachings fail to teach that a domain name is reserved for secure communication links. The Patent Owner provides no substantive analysis, simply making the conclusory statement that Aziz does not teach the claim limitation. To the extent that the Patent Owner's argues that Aziz does not use the specific word "reserved," the argument fails because the prior art is not required to use the identical words used in the claim. (*See* MPEP 2131 ("The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required.").)

The Patent Owner, in merely parroting the claim language, fails to explain how the limitations of the claims are in any way different from the disclosure of Aziz. As such, the Patent Owner's response fails to "distinctly and specifically points out the supposed errors in the examiner's action" and is instead merely a "general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references." (37 C.F.R. § 1.111(b).)

The Examiner's rejection is proper and should be made final.

g. Dependent Claims 24 and 48

The Examiner properly rejected claims 24 and 48 because Aziz teaches:

- Organizing domain names "into smaller segments, which are referred to as 'zones' (e.g., eng.sun.com and corp.sun.com)." (Aziz, 1:58-60.)
- Each zone "has its own database (the 'zone database') containing the names, addresses, and other information for the machines in that zone." (Aziz, 1:66-68.)

- Access to a zone can be restricted such that computers within zone are not publicly visible, in which case the zone is a "protected zone." (Aziz, 2:20-22.)
- It is desirable to permit "authorized clients outside the protected zone to communicate with hosts inside the protected zone." (Aziz, 2:53-54.) To achieve this, a firewall is configured to handle "encrypted communications between authorized client 210 and machines inside protected zone 180." (Aziz, 9:5-7.)
- The firewall is a "secure exchanger," which is "a machine that handles secure communications for itself or for another machine (e.g., performs encryption or decryption)." (Aziz, 9:29-32 & 9:36-40.)

Accordingly, Aziz teaches that (i) unauthorized machines cannot resolve the domain names of machines in a protected zone, (ii) but authorized machines may communicate with the machines in the protected zone through a secure exchanger. Thus, Aziz teaches "wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link."

The Patent Owner argues, at pages 37-38, that "just because a machine is in a protected zone does not mean that the domain name of the machine comprises an indication that the domain name service system supports establishing a secure communication link." (Response at 38.) This argument fails because Aziz teaches that the machine names are correlated with their zones: "Oftentimes, an organization divides its domain into smaller segments, which are referred to as 'zones' (e.g., eng.sun.com and corp.sun.com)." (Aziz, 1:58-60.) Aziz further teaches that each zone is a "subdivision of the domain." (Aziz, 1:62.) A zone is not merely a group of computers; it is also the portion of the domain namespace associated with that group of computers. Thus, the name of a protected zone—which can only be resolved by authorized clients—is an "indication that the domain name service system supports establishing a secure communication link" as recited in claims 24 and 48.

The Examiner's rejection is proper and should be made final.

h. Dependent Claim 50

Requester inadvertently proposed to reject claim 50 as anticipated by Aziz. The proposed rejection refers to analysis of claim 26, and therefore should have been grouped together with the analysis and proposed rejection of claim 26 as obvious over Aziz in view of Lawton. Consistent with the analysis in the Request—which the Patent Owner does not contest—claim 50 should be

rejected as obvious over Aziz in view of Lawton.

i. Dependent Claims 2, 6, 7, 14, 15, 19-22, 24, 25, 27, 33-40, 43-46, 49, 51, 52, 58 & 59

The Patent Owner concedes that Aziz teaches the additional limitations recited in claims 2, 6, 7, 14, 15, 19-22, 24, 25, 27, 33-40, 43-46, 49, 51, 52, 58 & 59. Because these claims' respective parent claims are anticipated by Aziz, as shown above, the rejection of these claims should be reaffirmed and made final.

3. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1, 2, 5-9, 14-25, 27, 28, 33-52, and 57-60 Under 35 U.S.C. § 103(a) Based on Aziz (Issue 10)

The Examiner properly rejected claims 1, 2, 5-9, 14-25, 27, 28, 33-52, and 57-60 because Aziz renders obvious the limitations in these claims. The Patent Owner does not point to any specific limitation regarding the obviousness rejections. But in refuting the corresponding anticipation rejections, the Patent Owner repeatedly asserts that Aziz's SX, KEY, and SIG records—which support the establishment of security communication links—"include no indication about the capabilities of *the alleged domain name service system itself*." (Response at 31.) In short, the Patent Owner effectively concedes that Aziz teaches all of the claim limitations, but argues that Aziz's domain name servers do not include security records *for themselves*.

This argument depends on the Patent Owner's improper attempt to rewrite claim 1 to recite a "domain name service ~~system~~ server" through attorney argument. (See discussion above.) The Patent Owner's assertion that *only* outside NS 120 can be part of the claimed "system" is without merit. At a minimum, all of Aziz's name servers, including outside NS 120 and inside NS 130, are properly part of Aziz's "domain name service system." Aziz illustrates, in Fig. 6B, an example response providing an SX record for inside NS 130. (Aziz, 12:6-14.)

Furthermore, as explained above in the Requester's Comments regarding anticipation, Aziz teaches "Tasks ... to configure outside NS 120 include defining an SX resource record type and adding appropriate records to the name server database ***for outside NS 120***." (Aziz, 8:66-9:2.) Thus, Aziz provides an express suggestion to create security records that enable security communication links with the outside NS 120. Aziz also teaches that a secure exchanger is a "machine that handles secure communications for itself." (Aziz, 6:30.) To the extent that Aziz does not anticipate the claims, Aziz suggests that a domain name server can have security

records defined to allow it to participate in a secure communication link, and further that the domain name server may handle the secure communications itself. In view of these teachings, it would have been obvious to one of ordinary skill in the art to combine the functionality of Aziz's domain name server and the secure exchanger.

Accordingly, Aziz renders obvious claims 1, 2, 5-9, 14-25, 27, 28, 33-52, and 57-60. The Examiner's rejection is proper and should be made final.

4. Response to Patent Owner's Arguments Regarding the Rejection of Claims 3, 4, & 26 Under 35 U.S.C. § 103(a) Based on Aziz in View of Lawton (Issue 11)

a. Claims 3 & 4

The Patent Owner argues, at page 40, that Lawton fails to teach the "indication" limitation of parent claim 1. However, "[o]ne cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Aziz—not Lawton—to teach the "indication" limitation. The Patent Owner's argument is without merit.

b. Claim 26

The Examiner properly rejected claim 26 because Aziz and Lawton teach:

- Segregating a portion of network as a "protected zone." (Aziz, 5:11-18.)
- Providing an authorized client outside the protected zone to access to machines within the protected zone using encrypted communications. (Aziz, 9:5-9.)
- Connecting an "outside" name server to the network outside of the protected zone, and connecting a second "inside" name server within the protected zone. (Aziz, 5:11-18.)
- Creating an "alternative domain name server" so that business can "establish your own top-level domain." (Lawton, p. 1.)
- Alternate DNS extensions could include ".med, .xxx and .ltd" top-level domains. (Lawton, p. 1.)

Accordingly, Aziz and Lawton teach (i) using a domain name to refer to a protected zone of computers; (ii) providing secure access to the protected zone of computers; and (iii) using specialized domain names to refer to computers. Thus, it would have been obvious that a domain name "enables establishment of a secure communication link."

The Patent Owner argues, at pages 40-42, that "Aziz is silent regarding non-standard

domain names." (Response at 41.) However, the Patent Owner's argument about "standard" versus "non-standard" domain names is not relevant. The Patent Owner has provided no definition of a "standard" or a "non-standard" domain name. Claim 26 simply recites a "domain name." Aziz discloses that a domain name (e.g., corp.sun.com) enables establishment of a secure communication link.

The Patent Owner argues that Lawton "does not disclose that 'having a non-standard domain name such as that taught by Lawton' would require a connection to an inside NS within a protected zone." (Response at 41.) This argument is an improper attempt to show "nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Aziz—not Lawton—to teach the connection to an inside name server within a protected zone. Lawton teaches the use of non-standard domain names. The combination of Aziz and Lawton renders obvious the use of both standard and non-standard domain names that "enable[] establishment of a secure communication link."

The Patent Owner further argues that "*Lawton* does not disclose or suggest any connection between the alternative DNS extensions and the attributes of the servers that they identify." (Response at 42.) But a connection was well-known to those of skill in the art. For example, it was well-known that domain names beginning with "www" frequently correspond to servers participating in the World Wide Web and therefore providing HTTP communication service.[2] As such, those of skill in the art recognized that a domain name could indicate the communications capabilities of the server associated with the domain name.

The Patent Owner's argument is without merit.

5. Response to Patent Owner's Arguments Regarding the Rejection of Claim 9 Under 35 U.S.C. § 103(a) Based on Aziz in View of Franaszek (Issue 12)

a. Aziz and Franaszek Disclose All of the Features of Claim 9

The Examiner properly rejected claim 9 because Aziz and Franaszek teach:

[2] See, for example, Pfaffenberger generally, and the example server names in Request Ex. D-13 at 1553 (including "www.qmw.ac.uk" for a web server, "gopher.qmw.ac.uk" for a gopher server, and "ftp.qmw.ac.uk" for a file transfer protocol (FTP) server) and at 1555 (listing URLs for various medical journals, with most of their respective servers' names beginning "www").

- Organizing a network topology, for example, by segregating a portion of network as a "protected zone." (Aziz, 2:47-54 & 5:11-18.)
- Providing an authorized client outside the protected zone to access to machines within the protected zone using encrypted communications. (Aziz 9:5-9.)
- Organizing a plurality of networks into a hierarchy. (Franaszek, Abstract.)

Accordingly, it would have been obvious to organize the virtual private networks, as taught by Aziz, into a hierarchy as taught by Franaszek. The combination renders obvious "wherein the virtual private network is one of a plurality of secure communication links in a hierarchy of secure communication links" as recited in claim 9.

The Patent Owner argues, at page 43, that "Aziz does not disclose a hierarchy of secure communication links." (Response at 43.) The Patent Owner agrees that "Franaszek discloses '[a] hierarchy of multiple networks," but argues that "Franaszek does not disclose that any of multipath networks ... are secure communication links." (Response at 43.)

The Patent Owner's argument is an improper attempt to argue the references individually. "One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Aziz—not Franaszek—to teach a plurality of secure communication links. And the Examiner relied on Franaszek to teach organizing a plurality of communication paths into a hierarchy. The Patent Owner's argument is without merit.

b. Aziz and Franaszek Are Readily Combinable

The Patent Owner argues, at pages 43-45, that the combination of Aziz and Franaszek is improper because "it would require the computer networks of Aziz to be modified to accommodate hardware components traditionally used for connecting processors and memories within a shared-memory computer," that is, to accommodate the devices of Franaszek. (Response at 45.)

This argument fails because the "test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference." (MPEP 2145(III).) Franaszek's multistage networks do not need to be bodily incorporated into Aziz's secure communication network, as the Patent Owner argues. Here, Franaszek teaches organizing computer communication paths into a hierarchy of communication networks. It would have been obvious to apply the known technique of organizing communication paths into

a hierarchy—as taught by Franaszek—to the similar communication system of Aziz, thereby improving the system of Aziz in the same way. (*See* MPEP § 2143 ("Exemplary rationales that may support a conclusion of obviousness include: … (C) Use of known technique to improve similar devices (methods, or products) in the same way").)

The Examiner's rejection is proper and should be made final.

c. One of Ordinary Skill in the Art Would Have Relied on Aziz and Franaszek

The Patent Owner argues, at page 45-56, that Franaszek is nonanalogous art because it "does not provide any information whatsoever about making it easy and convenient to enable secure communications." (Response at 45.) The Patent Owner further states that the "hierarchy of multistage networks disclosed in Franaszek would have been useless in addressing the problems solved by the features recited in claim 9." (Response at 46.) This argument fails because claim 9 is directed to the same problem as Franaszek, e.g., organizing a plurality of communication links. It is irrelevant that Franaszek's communication links are not taught as being secure, since the Examiner's rejection did not rely on Franaszek for a security teaching.

To the extent that Patent Owner argues that claim 9 is directed to "easy and convenient" communications, the Patent Owner's argument fails because it is untethered from the claim language. Claim 9 recites "one of a plurality of secure communication links in a hierarchy of secure communication links." The Patent Owner makes no argument, and points to no corresponding disclosure in the '504 specification, showing how a hierarchical organization of secure communication links is pertinent to solving a need for "easy and convenient" communications.

Furthermore, the communication network in Franaszek is analogous to the communication network in in Aziz. Franaszek's network operates, in part, by transmitting data in packets that "contain[], in addition to data, control information, including the address of the desired destination." (Franaszek, 3:61-64.) The packets are provided to switches that look at the destination address and send the packet to the destination. (Franaszek, 3:65-4:9.) Thus, data transit the network over a "store-and-forward" mechanism whereby data are forwarded from one node to the next until they reach their destination. (Franaszek, 6:36-40.) Aziz's network—which uses Transmission Control Protocol (TCP) (Aziz, 2:40-44)—functions in the same way. TCP "intended for use as a highly reliable host-to-host protocol between hosts in ***packet-***

switched computer communication networks." (RFC 793 at 1 (emphasis added); *see id.* at 7-8.)

The Examiner's rejection was proper.

6. Response to Patent Owner's Arguments Regarding the Rejection of Claim 10 Under 35 U.S.C. § 103(a) Based on Aziz in View of Schneier (Issue 13)

The Patent Owner does not raise any argument regarding Schneier's teaching of the additional limitation of claim 10. The Patent Owner argues, at page 46, that Schneier fails to teach the "indication" limitation of claim 1. However, "[o]ne cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Aziz—not Schneier—to teach the "indication" limitation. The Patent Owner's argument is without merit.

7. Response to Patent Owner's Arguments Regarding the Rejection of Claims11-13 Under 35 U.S.C. § 103(a) Based on Aziz in View of Martin (Issue 14)

a. Claim 11

The Examiner properly rejected claim 11 because the prior art teaches that a client can choose from multiple source addresses when it transmits its communications. (Martin at 9.)

Accordingly, Aziz and Martin teach that when a client is initiating a new communication link to a server, the client can randomly choose the source ("from") address to be used. The addresses used can be different for each connection. Thus, the prior art teaches a "network address hopping regime that is used to pseudorandomly change network addresses in packets" as recited in the claim 11.

The Patent Owner argues, on pages 46-47, that Martin fails to teach the "indication" limitation of claim 1. However, "[o]ne cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Aziz—not Martin—to teach the "indication" limitation. The Patent Owner's argument is without merit.

The Patent Owner concludes, without explanation, that a regime for changing network addresses based on randomly selecting source addresses, as taught by Martin, is somehow different than "pseudorandomly chang[ing] network addresses in packets" as recited in claim 11. Randomly using different network addresses for each connection teaches that the source network addresses in the packets transiting the virtual private network randomly change. To the extent

that the Patent Owner believes that the claim has a different meaning, the Patent Owner has neither explained that meaning nor provided any reasoning for it. (*See* 37 CFR 1.111(b).)

The Examiner's rejection is proper and should be made final.

b. Claim 12

The Patent Owner argues that "*Martin* does not disclose a moving window of valid values." (Response at 47.) This argument fails because it does not account for the full scope of Martin's teachings to one of ordinary skill in the art.

Martin teaches that a "client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random subject to lanon uniqueness...." (Martin at 9.) The list from which the source address/port pair is chosen, A_{TCP}, is the "set of all possible TCP endpoint connection identifiers." (*Id.*) Although a source address/port pair is chosen at random, Martin teaches to ensure "uniqueness" for each connection, that is, that a chosen source address/port pair is not already in used for another connection. Thus, Martin in general teaches that although a plurality of source address/port pairs exists, only a subset are in use at any one time, and the list changes with every new connection. This list of active source address/port pairs is a "moving window of valid values." Accordingly, it would have been obvious when processing packets transmitted and received by the client, to compare the address and port number identified in the packet to the list of address/port pairs in active use. Thus, Aziz in view of Martin renders obvious "comparing a value in each data packet transmitted between a first device and a second device to a moving window of valid values" as recited in claim 12.

c. Claim 13

The Patent Owner argues that "*Martin* does not disclose a table of valid discriminator fields." (Response at 48.) This argument fails because it does not account for the full scope of Martin's teachings to one of ordinary skill in the art.

Martin teaches that a "client building an outbound TCP connection should select its source address/port pair from A_{TCP} at random subject to lanon uniqueness...." (Martin at 9.) The list from which the source address/port pair is chosen, A_{TCP}, is the "set of all possible TCP endpoint connection identifiers." (*Id.*) Although a source address/port pair is chosen at random, Martin teaches to ensure "uniqueness" for each connection, that is, that a chosen source address/port pair is not already in used for another connection. Thus, Martin in general teaches that although a plurality of source address/port pairs exists, only a subset are in use at any one

time, and the list changes with every new connection. This list of active source address/port pairs is a "table of valid discriminator fields." Accordingly, it would have been obvious when processing packets transmitted and received by the client, to compare the address and port number identified in the packet header to the list of address/port pairs in active use. Thus, Aziz in view of Martin renders obvious "a comparison of a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for a first device" as recited in claim 13.

8. Response to Patent Owner's Arguments Regarding the Rejection of Claims 29-32 & 53-56 Under 35 U.S.C. § 103(a) Based on Aziz in View of Ludwig (Issue 15)

The Patent Owner does not argue for the separate patentability of claims 29-32 and 53-56, relying instead on its arguments regarding parent claims 1 and 36. The Patent Owner also argues that Ludwig fails to disclose the "indication" limitations of claims 1 and 36, but "[o]ne cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Aziz—not Ludwig—to teach the limitations of claims 1 and 36. Since the Patent Owner's arguments are without merit, the rejection of claims 29-32 and 53-56 is proper and should be made final.

C. Kiuchi and Pfaffenberger

1. Overview of Kiuchi

"C-HTTP – The Development of a Secure, Closed HTTP-based Network on the Internet" by Takahiro Kiuchi and Shigekoto Kaihara ("Kiuchi") was published by IEEE in the Proceedings of the Symposium on Network and Distributed System Security, 1996. This publication was publicly available more than one year before the '504 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b).

Similar to the '504 patent, Kiuchi was concerned with establishing secure network links between computers. Kiuchi sought to develop a secure network by which medical information, including sensitive clinical trial documents, could be easily shared between different hospitals and other institutions. Kiuchi's secure network is built using the C-HTTP and HTTP protocols.

Kiuchi teaches that a secure C-HTTP name service stores domain names and corresponding addresses. This stored information is used to respond to queries from clients seeking to establish a secure communication link with servers.

2. Overview of Pfaffenberger

"Netscape Navigator 3.0: Surfing the Web and Exploring the Internet," by Bryan Pfaffenberger, is a book published by Academic Press in 1996. This publication was publicly available more than one year before the '504 Patent's earliest claimed priority date of October 30, 1998 and is prior art under 35 U.S.C. § 102(b).

Pfaffenberger describes Netscape Navigator, which at the time was the most popular HTTP client software (also referred to as a web browser). Because of this popularity, it would have been obvious to use the Netscape Navigator software as an HTTP client in Kiuchi's system. Pfaffenberger teaches that HTTP client software can provide a visual indication to a user of whether a communication link to a server is secure.

3. Response to Patent Owner's Arguments Regarding the Rejection of Claims 1-4, 6, 8-10, 12-19, 22, 24-30, 33, 34, 36-43, 46, 48-54, and 57-60 Under 35 U.S.C. § 103(a) Based on Kiuchi in View of Pfaffenberger (Issue 16)

As set forth in the Request and in the comments below, the Examiner's rejections are proper and therefore should be made final.

a. Independent Claim 1

The Examiner correctly determined that Kiuchi and Pfaffenberger teach multiple independent "indications" that the disclosed domain name service system supports establishing a secure communication link, as analyzed more completely below.

(i) The C-HTTP Name Server Returning the Public Key of the Server-Side Proxy is an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link."

The Examiner correctly determined that Kiuchi and Pfaffenberger render obvious an "indication that the domain name service system supports establishing a secure communication link" because Kiuchi and Pfaffenberger teach:

- A domain name service system that includes a "C-HTTP name server." (Kiuchi at 64.)
- "The C-HTTP name server manages … the public keys of all proxies which participate in the closed network." (Kiuchi at 65.)
- The C-HTTP name server receives a request from the client to communicate with the server, and the C-HTTP name server uses the information about the server to retrieve the

server's public key: "A client-side proxy asks the C-HTTP name server whether it can communicate with the host ... If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy." (Kiuchi at 65).

- The communications between and among the C-HTTP name server, client-side proxy, and server-side proxy are encrypted. (Kiuchi, Abstract at 64.)
- At a user's HTTP client software, a "Doorkey Icon... indicates whether you're accessing a secure server." (Pfaffenberger at 13.)

Accordingly, Kiuchi discloses that (i) the C-HTTP name server is a central computer; (ii) the centralized C-HTTP name server maintains the IP addresses and public keys for each computer that participates in the closed network, (iii) the C-HTTP name server determines whether a connection is permitted, and (iv) the C-HTTP server, using the information about a server as supplied by a client, retrieves the corresponding IP address and public key of the server. Pfaffenberger further teaches providing a visual indication to a user regarding whether a communication link to a server is secure. Therefore, Kiuchi and Pfaffenberger render obvious an "indication that the domain name service system supports establishing a secure communication link" as recited in claim 1.

The Patent Owner argues, at pages 51-52, that "the public key corresponds to the server-side proxy, which is separate from the alleged domain name service system, the C-HTTP name server." This argument fails to take into account for the full disclosure of Kiuchi.

Kiuchi expressly teaches that the secure C-HTTP name server participates in secure communication links with both the client- and server-side proxies. For example, "asymmetric key encryption [is used] for the secure exchange of ... host information between a proxy and C-HTTP name server." (Kiuchi at 64.) Kiuchi provides, on pages 72-73, a detailed explanation of the protocol used to communicate between the proxies and the secure C-HTTP name server. In the protocol definition, "lines with an asterisk are encrypted." (Kiuchi at 72.) Numerous items in the requests from both the client-side proxy and the server-side proxy are encrypted:

2. Communications between a client-side proxy and C-HTTP name server

2.1 C-HTTP name service request

C-HTTP-NAME-SERVICE-VERSION<CR><LF>
ENCRYPTION-ALGORITHM<CR><LF>
ENCRYPTED-PART-LENGTH<CR><LF>
SIGNATURE-ALGORITHM<CR><LF>
SIGNATURE-LENGTH<CR><LF>
MESSAGE-DIGEST-ALGORITHM<CR><LF>
<CR><LF>
*REQUEST-TYPE<CR><LF>
*CLIENT-SIDE-PROXY-IP<CR><LF>
*USER-AGENT-IP<CR><LF>
*SERVER-SIDE-PROXY-NAME<CR><LF>
*SERVER-SIDE-PROXY-PORT<CR><LF>
<CR><LF>
*DIGITAL-SIGNATURE

3. Communications between a sever-side proxy and C-HTTP name server

3.1 C-HTTP name request

C-HTTP-NAME-SERVICE-VERSION<CR><LF>
ENCRYPTION-ALGORITHM<CR><LF>
ENCRYPTED-PART-LENGTH<CR><LF>
SIGNATURE-ALGORITHM<CR><LF>
SIGNATURE-LENGTH<CR><LF>
MESSAGE-DIGEST-ALGORITHM<CR><LF>
<CR><LF>
*REQUEST-TYPE<CR><LF>
*SERVER-SIDE-PROXY-IP<CR><LF>
*SERVER-SIDE-PROXY-PORT<CR><LF>
*CLIENT-SIDE-PROXY-NAME<CR><LF>
*USER-AGENT-IP<CR><LF>
<CR><LF>
*DIGITAL-SIGNATURE

(Kiuchi at 72-73.) Kiuchi also teaches that many items in the response sent by the secure C-HTTP name server are also encrypted. (*Id.*)

Thus, Kiuchi teaches that a domain name service system *itself* participates in a secure a secure communication link. Even under the Patent Owner's asserted interpretation, Kiuchi teaches the claim limitation.

The Patent Owner then continues by comparing Kiuchi's disclosure to the admitted prior art in the '504 patent specification. Absent from this comparison, however, is analysis comparing Kiuchi's disclosure to the claim limitation at issue. Kiuchi teaches not only name resolution capabilities, but also indications of support for establishing a security communication link (e.g., engaging in encrypted communications and returning a network address corresponding to a secure domain). Patent Owner's analysis of the two prior art systems—without addressing the Kiuchi's teaching of an "indication"—is not relevant.

The Examiner's rejection of claim 1 is proper and should be made final.

(ii) The C-HTTP Name Server Returning the IP Address of the Server-Side Proxy is an "Indication That the Domain Name Service System Supports Establishing a Secure Communication Link."

The Patent Owner argues, on pages 52-53, that the "IP address is for the server-side proxy" and "includes no indication about the capabilities of the C-HTTP name server itself." This argument fails to take into account the full disclosure of Kiuchi.

Kiuchi expressly teaches that the secure C-HTTP name server participates in secure, encrypted communication links with both the client- and server-side proxies. (See discussion,

supra, at page 35.) Thus, Kiuchi teaches the claimed "indication" under the Patent Owner's improper interpretation of the claim.

The Patent Owner then continues by comparing Kiuchi's disclosure to the admitted prior art in the '504 patent specification. Absent from this comparison, however, is analysis comparing Kiuchi's disclosure to the claim limitation at issue. Kiuchi teaches not only name resolution capabilities, but also indications of support for establishing a security communication link (e.g., engaging in encrypted communications and returning a network address corresponding to a secure domain). Patent Owner's analysis of the two prior art systems—without addressing the Kiuchi's teaching of an "indication"—is not relevant.

The Examiner's rejection of claim 1 is proper and should be made final.

(iii) Response to Patent Owner's Argument that Pfaffenberger Does Not Remedy the Deficiencies of Kiuchi

Pfaffenberger describes the most popular HTTP client[3] around the time of Kiuchi's disclosure, Netscape Navigator. One feature of this software is a Doorkey Icon that provides an indication to the end user of whether a server supported establishing a secure communication link. The Examiner properly relied on Pfaffenberger's disclosure as a further teaching of the claimed "indication" limitation.

The Patent Owner argues, at pages 53-55, that Pfaffenberger "does not indicate, specifically, that any purported domain name service system in Pfaffenberger supports establishing a secure communication link." (Response at 54.) This argument fails because the Examiner's rejection did not rely on Pfaffenberger as teaching a domain name service system. "One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) The Examiner properly determined that Kiuchi teaches a "domain name service system" and that Pfaffenberger teaches indicating whether a server supports secure communications. Accordingly, Kiuchi and Pfaffenberger render obvious an "indication that the domain name service system supports establishing a secure communication link" as recited in the claim.

[3] *See* Request Ex. D-13 at 1554 ("Although Mosaic revolutionized the web, it has now been replaced by Netscape Navigator as the most commonly used web browser.").

(iv) Response to Patent Owner's Argument that One of Ordinary Skill in the Art Would Not Have Relied on Pfaffenberger

The Patent Owner argues that Pfaffenberger is nonanalogous art because it is not directed to the problem of "mak[ing] it easy and convenient to enable secure communications." (Response at 55.) This argument is without merit.

First, Pfaffenberger describes the most popular HTTP client around the time of Kiuchi's disclosure.[4] Kiuchi is directed to a communication system built, in part, using HTTP clients. Thus, one of ordinary skill in the art would have looked to Pfaffenberger and Netscape Navigator in working with the HTTP clients in Kiuchi's system.

Second, Pfaffenberger is highly relevant to the problem of enabling convenient and secure communication links. Pfaffenberger's Doorkey Icon provides an imminently convenient way to indicate to a user whether a communication link is secure. Pfaffenberger also teaches the importance of a user's awareness that a particular communication link is secure, for example, so that the user can avoid transmitting sensitive information over an insecure communication link: "Don't give your credit card number to any on-line vendor unless the connection is secure!" (Pfaffenberger at 13.)

Thus, the Examiner correctly rejected claim 1 as rendered obvious by Kiuchi in view of Pfaffenberger. The Rejection should be made final.

b. Independent Claims 36 & 60

Regarding independent claims 36 and 60, the Patent Owner's relies on the same improper and erroneous arguments related to claim 1 that are refuted above. Accordingly, the rejections of claims 36 and 60 should be reaffirmed and made final.

c. Dependent Claims 8, 9, 10, 12 & 13

The Examiner correctly rejected claim 8 because Kiuchi teaches:

- The secure HTTP communication mechanism is used for private network communication: "'C-HTTP' [] provides secure HTTP communication mechanisms within a closed group of institutions on the Internet." (Kiuchi at 64); "[S]ome medical information has to be shared among some hospitals, but it should not be made available

[4] *See* Request Ex. D-13 ("Although Mosaic revolutionized the web, it has now been replaced by Netscape Navigator as the most commonly used web browser.").

to other sites." (Kiuchi at 64.)

- The secure HTTP communication is a separate, virtual network on top of the Internet for the closed group of institutions: "[W]e discuss the design and implementation of a closed HTTP (Hypertext Transfer Protocol)-based network (C-HTTP) **which can be built on the Internet**." (Kiuchi at 64, emphasis added); "C-HTTP is assumed to be used in **a closed group of institutions on the Internet**, in which each member is protected by its own firewall." (Kiuchi at 64, emphasis added.)

Accordingly, Kiuchi discloses: (i) an encrypted communication link (C-HTTP) to facilitate communication within a closed group of institutions on the Internet (e.g., private network communication link); (ii) the private network communication link is a virtual network built on top of the Internet; (iii) the C-HTTP name server is connected to and a part of the virtual network. Thus, Kiuchi teaches that the "domain name service system is connectable to a virtual private network through the communication network" as recited in claim 8.

The Patent Owner does not respond to the Examiner's rejection, but instead submits arguments, on pages 56-63, premised on the contention that "the C-HTTP connection in *Kiuchi* corresponds to the virtual private network recited in claim 8." (Response at 56.) But this is not correct. The Examiner's rejection identified, as a "virtual private network," Kiuchi's teaching of a "Secure, Closed HTTP-based Network on the Internet" based on "requests and responses transmitted among the C-HTTP name service, the client-side proxy, and the server-side proxy." (Request, Ex. F-3 at 15.) Kiuchi also teaches that the disclosed C-HTTP name server and proxies can be used to create "a closed HTTP-based ***virtual network***." (Kiuchi at 69 (emphasis added).) Thus, the "virtual private network" includes all of the computers participating Kiuchi's closed HTTP-based virtual network.

Because all of the Patent Owner's subsequent arguments are based on this misunderstanding of the Examiner's rejection, the arguments are moot and without merit. Nevertheless, Requester provides the following additional comments on the Patent Owner's misdirected response.

The Patent Owner attempts to inject a particular definition of "virtual private network" by citing to the declaration of Dr. Angelos Keromytis as support for this definition. Neither the Patent Owner nor Dr. Keromytis, however, cite to any such express definition in the specification of the '504 Patent. The Patent Owner, on pages 56-57, describes a particular

implementation of a virtual private network involving A, B, X, and Y, and then concludes "Kiuchi fails to disclose such a virtual private network." (Response at 57 (emphasis added).) By describing the very narrow description of a virtual private network involving A, B, X, and Y, Patent Owner is advancing a new, narrow interpretation of "virtual private network" that does not appear in the claims of the '504 patent. This is improper, because claims are to be given their broadest reasonable interpretation in light of the supporting disclosure. (*See* MPEP 2106; *In re Morris*, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997).)

Kiuchi discloses a virtual private network and it is not relevant whether Kiuchi discloses a particular and specific implementation of a virtual private network that is not recited in the claims. Kiuchi discloses a domain name server that enables secure communication among a closed group of institutions over the Internet (*e.g.*, a virtual private network). Accordingly, Kiuchi teaches that "the domain name service system is connectable to a virtual private network through the communication network" as recited in the claim.

Patent Owner further argues, on pages 57-58, that Kiuchi uses a point-to-point connection, and thus, the point-to-point connection of Kiuchi could not anticipate the claimed virtual private network communication link. Patent Owner's argument is attempting to introduce new limitations and subjective ambiguity into the claims, which is not permissible. MPEP 2106; *E-Pass Techs., Inc. v. 3Com Corp.*, 343 F.3d 1364, 1369, 67 USPQ2d 1947, 1950 (Fed. Cir. 2003). Patent Owner is introducing new limitations by arguing that the recited virtual private network communication link is not implemented via point-to-point connections. The claims simply recite a "virtual private network," and introducing a new limitation regarding *a specific implementation* of a virtual private network (that is not described in the specification), such as a "virtual private network implemented not via point-to-point links" would be erroneous.

Moreover, Patent Owner's expert's self-serving statements that secure point-to-point communications cannot be a virtual private network does not comport with the knowledge known to those of ordinary skill in the art. For example, Exhibit G and Exhibit H show that it was publicly known at the time of the invention that virtual private networks could be implemented via point-to-point links.[5]

[5] *See* Exhibit G (Malkin), pg. 20 ("For example, the IETF recently began considering the Layer 2 Tunneling protocol (L2TP), which combines Microsoft's Point-to-Point Tunneling protocol and

The Patent Owner argues, on page 58, that Kiuchi's virtual private network "does not include the alleged *domain name service system*, the C-HTTP name server." (Response at 58.) The Patent Owner's argument attempts to introduce another new limitation into the claim, which is not permissible. The Patent Owner attempts to limit the claim to virtual private networks that *include* the domain name service system. The claim instead recites that the domain name service system is "connectable to a virtual private network." Introducing a new limitation, such as "wherein the domain name service system is part of the virtual private network," would be erroneous.

Furthermore, as noted above, the Examiner properly identified Kiuchi's "closed HTTP-based virtual network" of institutions over the Internet as the virtual private network. This virtual network *includes* the closed-HTTP (C-HTTP) name server. Even under the Patent Owner's asserted interpretation of the claim, Kiuchi teaches that the C-HTTP name server is "connectable to a virtual private network."

Accordingly, the Patent Owner's arguments (i) are not responsive to the Examiner's rejection (ii) attempt to introduce a definition not supported by the specification, (iii) do not reflect the broadest reasonable interpretation of the claim language, (iv) attempt to improperly introduce new limitations into the claim, and (v) contradict publicly available information known about virtual private networks.

The Examiner's rejection was proper.

a. Dependent Claim 9

The Patent Owner does not raise any argument specific to claim 9, and as such, concedes that Kiuchi and Pfaffenberger render obvious the additional limitation of claim 9. The Examiner's rejection is proper and should be made final.

b. Dependent Claim 10

The Examiner properly rejected claim 10 because Kiuchi teaches:

Cisco Systems' Layer 2 Forwarding protocol. L2TP would permit users with protocol-compliant hardware and software vendors to work across the same VPN [virtual private network].").
See Exhibit H (Ortiz, Jr.), pg. 555 ("Consider the topology shown in figure 1. It illustrates a Service Provider's network that the corporate Network uses for Dial-in Virtual Private Network server. A Layer 2 solution would establish a Point-to-Point Protocol (PPP) connection...").

- that "request" and "response" packets (e.g., data packets) are sent to and from the C-HTTP name server; (Kiuchi at 72-73.)
- each of these data packets have random values inserted into them: "[r]andom bytes inserted every fourth byte of the request and response before encryption in order to avoid the same encrypted requests or responses being repeated;" (Kiuchi at 72.) and
- The "C-HTTP name server provides both client-side and server-side proxies with each peer's public key." (Kiuchi at 65.) Thus, the "request" and "response" packets are necessary to create the virtual private network (e.g., the virtual private network of Kiuchi is based on these data packets).

Accordingly, Kiuchi discloses: (i) establishing a virtual private network by first transmitting request and response packets; and (ii) inserting random bytes into communications between the proxies and the secure C-HTTP name server to further obscure their contents. It would have been obvious to further use the disclosed technique of inserting random bytes into the communications between the two proxies for the same purpose. Therefore, Kiuchi renders obvious that the "virtual private network is based on inserting into each data packet communicated over a secure communication link one or more data values that vary according to a pseudo-random sequence."

Patent Owner argues that, because Kiuchi discloses that the random bytes are inserted into name requests and "not into C-HTTP communications," then Kiuchi cannot teach "the virtual private network is based on inserting into each data packet" limitation. This argument fails because, as noted above with respect to claim 8, the Examiner's rejection identified, as the claimed virtual private network, Kiuchi's "closed HTTP-based virtual network" (Kiuchi at 69) based on "requests and responses transmitted among the C-HTTP name service, the client-side proxy, and the server-side proxy." (Request, Ex. F-3 at 15.) Thus, the "virtual private network" includes all of the computers participating Kiuchi's closed HTTP-based virtual network, including the C-HTTP name server.

Furthermore, explicit disclosures are not required and the prior art is not to be considered in a vacuum but, "together with the knowledge of one of ordinary skill in the pertinent art'...at the time the...patent was filed." (*In re Paulson*, 30 F.3d 1475, 1480; *see also, In re Baxter Travenol Labs*, 952 F.2d 388, 391.) It would have been obvious to use the disclosed technique of inserting random bytes into the communications between the two proxies for the same reason

that the random bytes are inserted into the communications between a proxy and the secure C-HTTP name server. Thus, the Examiner's obviousness reject is proper.

c. Dependent Claim 12

The Patent Owner argues, on page 61, that "Kiuchi does not explain how the values of the Nonce header field are checked" and that "there are many ways that the values of the Nonce header field could be checked without comparing them to a moving window of valid values." The Patent Owner is incorrect.

Kiuchi discloses a "moving window of valid values" because the Nonce values of Kiuchi are values that indicate where a packet belongs in a message sequence, and the Nonce values are checked to prevent attacks. Kiuchi discusses an example sequence involving a number of requests and responses. The Nonce values from those requests and responses are below:

Request-Nonce	Response-Nonce
8abd853f	ef23dc99
8abd8540	ef23dc9a
8abd8541	ef23dc9b

(*See* Kiuchi, 74-75.)

Patent Owner makes the strange argument that the "same request and response Nonce values are sent to both the client-side proxy and the server-side proxy." However, Kiuchi is clear: the Nonce values are a *sequence of hexadecimal-based numbers* (e.g., "...3f...40...41" and "99...9a...9b") that are verified to prevent replay attacks.

Further, Patent Owner's arguments contradict the specification of the '504 patent, which provides a definition of a "moving window of valid values": "1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence." ('504 Patent, 11:46-48.)

Accordingly, (i) Kiuchi discloses an identifier that indicates where the packet belongs in the message sequence, and (ii) the specification of the '504 patent defines a window sequence number as an identifier that indicates where the packet belongs in the original message sequence. Thus, Kiuchi's message sequence identifiers are a "moving window of valid values."

The Patent Owner also argues, on page 61, that Kiuchi's requests and responses are not "data packets," citing only to the declaration of Dr. Keromytis. Neither the Patent Owner nor Dr. Keromytis, however, cite to any definition of "data packets" in the specification of the '504

Patent. Accordingly, the Patent Owner has no support for its assertion that the term "data packets" has a specialized meaning that would distinguish the data transmissions in Kiuchi.

d. Dependent Claim 13

On page 62, Patent Owner also argues that Kiuchi does not teach that the Nonce values are compared to a "table of valid discriminator fields." Patent Owner is incorrect.

Kiuchi discloses a "table of valid discriminator fields" because Kiuchi teaches that the current Nonce value is compared against the previous Nonce values to verify that the proper sequence of Nonce values are transmitted. Thus, the previously received values represent the "table of valid discriminator fields" and the current Nonce value is compared against that table of valid discriminator fields.

Further, there is nothing recited in the claims that define the size or content of the "table of valid discriminator fields." There is nothing recited in the claims about what type of comparison is performed (equal to, less than, more than) against the "table of valid discriminator fields." Accordingly, Kiuchi discloses that a current Nonce value is compared against the previous Nonce values (e.g., a table of valid discriminator fields) as recited in the claims.

Patent Owner repeats the argument that the C-HTTP responses and responses do not qualify as the recited "data packets." However, as discussed above, the claims are silent as to any detail about the data packets, and it would be improper to import limitations into the claim about the type, manner, purpose, or sending and receiving of the data packets. Kiuchi discloses data packets (the "request" and "response" packets sent to and from the C-HTTP name server protocol). Accordingly, Patent Owner's argument is without merit.

The Examiner's rejection was proper.

e. Dependent Claims 17 & 41

The Patent Owner does not argue for the separate patentability of the claim limitations recited in claims 17 and 41, relying instead on its arguments regarding parent claims 1 and 36. Since the Patent Owner's arguments are without merit, the rejection of claims 17 and 41 is proper and should be made final.

f. Dependent Claims 24 & 48

The Patent Owner argues, on pages 63-64, that "the status of the server indicates nothing regarding the capabilities of the alleged domain name service system, the C-HTTP name server."

The Patent Owner is incorrect.

Kiuchi teaches that an example domain name for a C-HTTP name server is "Name.Server.CSCRG". (Kiuchi at 73, col. 2.) This name is not valid in the general Internet domain name system, and instead is valid only in the secure C-HTTP closed network. Accordingly, the name server's domain name is "an indication that the domain name service system supports establishing a secure communication link," as recited in claims 24 and 48.

g. Dependent Claim 26

The Patent Owner argues, at page 64, that Kiuchi's teaching to use domain names to establish secure communication links differs somehow from the claim limitation that a domain name "enables establishment of a secure communication link." The Patent Owner is incorrect.

Kiuchi teaches that a client-side proxy provides a domain name to the C-HTTP name server as part of the process of establishing a secure communication link. Thus, the domain name "enables establishment of a secure communication link" as recited in the claim.

h. Dependent Claim 27

The Patent Owner argues, at page 65, that "Kiuchi's C-HTTP closed network ... does not demonstrate anything about what the alleged *domain name service system*, the C-HTTP name server, is configured to do." (Response at 65.) The Patent Owner is improperly attempting to rewrite claim 1 to recite a "domain name service ~~system~~ server" through attorney argument. The Patent Owner's assertion that the claimed "system" must be found in a single server is unfounded. As previously noted, the '504 specification repeatedly uses the word "system" to refer to a collection of multiple components.

As such, the Patent Owner fails to respond to the Examiner's rejection. The Examiner's rejection showed, for example, how Kiuchi's C-HTTP name server enables a user at the Tokyo Branch Hospital (a "first location") to establish a secure communication link to a server at Coordinating.Center.CSCRG (a "second location"). (Ex. F-3 at 32.) The Examiner also highlighted Kiuchi's teaching that its secure protocol is "transparent" so that "[e]nd-users do not have to employ security protection procedures." (Ex. F-3 at 33; Kiuchi at 68.) Thus, Kiuchi teaches a "domain name service system is configured to enable establishment of a secure communication link between a first location and a second location transparently to a user at the first location" as recited in claim 27.

The Examiner's rejection is proper.

i. Dependent Claims 2-4, 6, 7, 11, 14-16, 18, 19, 22, 25, 28-30, 33, 34, 37-40, 42, 43, 46, 49-54, & 57-59

The Patent Owner does not argue for the separate patentability of claims 2-4, 6, 7, 11, 14-16, 18, 19, 22, 25, 28-30, 33, 34, 37-40, 42, 43, 46, 49-54, and 57-59, relying instead on its arguments regarding parent claims 1 and 36. As such, the Patent Owner concedes that Kiuchi and Pfaffenberger render obvious the additional limitations recited in these claims. The rejection of these claims is proper and should be made final.

4. Response to Patent Owner's Arguments Regarding the Rejection of Claims 5, 23, & 47 Under 35 U.S.C. § 103(a) Based on Kiuchi in View of Pfaffenberger and Rivest (Issue 17)

The Patent Owner does not argue for the separate patentability of claims 5, 23, and 47, relying instead on its arguments regarding parent claims 1 and 36. The Patent Owner does argue that Rivest fails to disclose the "indication" limitations of claims 1 and 36, but "nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Kiuchi and Pfaffenberger—not Rivest—to teach the limitations of claims 1 and 36. Since the Patent Owner's arguments are without merit, the rejection of claims 5, 23, and 47 are proper and should be made final.

5. Response to Patent Owner's Arguments Regarding the Rejection of Claim 7 Under 35 U.S.C. § 103(a) Based on Kiuchi in View of Pfaffenberger and Borella (Issue 18)

The Patent Owner does not argue for the separate patentability of claim 7, relying instead on its arguments regarding parent claim 1. The Patent Owner argues that Borella fails to disclose the "indication" limitation of claim 1, but "nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Kiuchi and Pfaffenberger—not Borella —to teach the limitations of claim 1. Since the Patent Owner's arguments are without merit, the rejection of claim 7 is proper and should be made final.

6. Response to Patent Owner's Arguments Regarding the Rejection of Claim 11 Under 35 U.S.C. § 103(a) Based on Kiuchi in View of Pfaffenberger and Martin (Issue 19)

The Patent Owner argues, on page 67, that Martin fails to teach the "indication" limitation of claim 1. However, "[o]ne cannot show nonobviousness by attacking references

individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Kiuchi and Pfaffenberger—not Martin—to teach the "indication" limitation. The Patent Owner's argument is without merit.

The Patent Owner concludes, without explanation, that a regime for changing network addresses based on randomly selecting source addresses, as taught by Martin, is somehow different than "pseudorandomly chang[ing] network addresses in packets" as recited in claim 11. Randomly using different network addresses for each connection teaches that the source network addresses in the packets transiting the virtual private network randomly change. To the extent that the Patent Owner believes that the claim has a different meaning, the Patent Owner has neither explained that meaning nor provided any reasoning for it. (*See* 37 CFR 1.111(b).)

The Examiner's rejection is proper and should be made final.

7. Response to Patent Owner's Arguments Regarding the Rejection of Claims 20, 21, 35, 44, & 45 Under 35 U.S.C. § 103(a) Based on Kiuchi in View of Pfaffenberger and Broadhurst (Issue 20)

The Patent Owner does not argue for the separate patentability of claims 20, 21, 35, 44, and 45, relying instead on its arguments regarding parent claims 1 and 36. The Patent Owner also argues that Broadhurst fails to disclose the "indication" limitation of claims 1 and 36, but "nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).) Here, the Examiner properly relied on Kiuchi and Pfaffenberger—not Broadhurst —to teach the limitations of claims 1 and 36. Since the Patent Owner's arguments are without merit, the rejection of claims 20, 21, 35, 44, and 45 is proper and should be made final.

8. Response to Patent Owner's Arguments Regarding the Rejection of Claim 31, 33, 35, & 56 Under 35 U.S.C. § 103(a) Based on Kiuchi in View of Pfaffenberger and Ludwig (Issue 21)

Requester proposed rejecting claims 31-32 and 55-56 as obvious over Kiuchi in view of Pfaffenberger and Ludwig. The Office Action, however, rejected claims 31, 33, 35, and 56 on this combination of references.

In any event, the Patent Owner does not contest that Ludwig discloses the additional limitations recited in these claims. The Patent Owner merely argues that Ludwig fails to disclose the "indication" limitation of claims 1 and 36, but "nonobviousness by attacking references individually where the rejections are based on combinations of references." (MPEP § 2145 (IV).)

Here, the Examiner properly relied on Kiuchi and Pfaffenberger—not Ludwig —to teach the limitations of claims 1 and 36. Since the Patent Owner's arguments are without merit, the Examiner's rejection should be made final.

D. Response to Patent Owner's Argument That Secondary Considerations Demonstrate Non-Obviousness

On page 69, Patent Owner argues that secondary considerations rebut any finding of obviousness. To be given substantial weight in determining obviousness or nonobviousness, evidence of secondary considerations must be relevant to the subject matter as claimed, and therefore the Examiner must determine whether there is a nexus between the merits of the claimed invention and the evidence of secondary considerations. MPEP 716.01(b). Further, in the absence of an established nexus with the claimed invention, secondary consideration factors are not entitled to much, if any, weight and generally have no bearing on the legal issue of obviousness. *See In re Vamco Machine & Tool, Inc.*, 752 F.2d 1564, 1577 (Fed. Cir. 1985).

First, Patent Owner has failed to establish any nexus between the '504 patent and the "evidence." Patent Owner points to a declaration by the inventor of the '504 that describes different government funding programs designed to promote science and technology. However, simply because a government agency funds programs for "Next Generation Internet" and "Dynamic Coalitions" does not establish a nexus between those programs and the actual claims of the '504 patent. In order for any such evidence to be given weight, if any, the Patent Owner must establish a nexus between the evidence and the claimed invention. Patent Owner has merely listed a number of government-funded programs, with a passing reference to "secure communications." Patent Owner has not established a nexus between this evidence **and the actual claims of the '504 patent**.

Second, Patent Owner argues that the claimed invention has achieved commercial success by noting that several companies have licensed the patent portfolio. However, **a portfolio license does not establish commercial success**. (*Ex parte NTP, Inc., Appeal 2008-004603, slip op. at 132 (BPAI Dec. 22, 2009)*. The Board of Patent Appeals and Interferences has set forth the evidence needed to support the use of a list of licensees as evidence of secondary considerations: (i) testimony from a licensee as to why the licensee took a license; (ii) whether the taking of the license was a business cost-benefit analysis with regarding to defending an infringement suit, as opposed to the actual merits of the invention; (iii) the number of entities

who refused to take a license and why; (iv) the terms of the licenses and whether the licenses were favorable to the licensee; (v) market information indicating the number of products that are sold under licenses and the number of products that are not under license; (vi) the structure and operation of the devices made by the licensees to determine if those products embody the reasons as to why the "invention" is advantageous over the prior, if at all; (vii) whether the licensee took the licenses for reasons substantively related to each and every one of the claims of the '504 patent; and (viii) a declaration from a representative of any of the licensees attesting to and praising the merits of the claimed invention. (*Ex parte NTP* at 132-134). Patent Owner has not provided any such evidence.

Patent Owner has merely provided a declaration by the inventor that describes government programs and portfolio licenses. Patent Owner has not established any nexus between this "evidence" and the actual claimed invention. Further, Patent Owner has not provided any of the evidence necessary to establish commercial success.

Accordingly, the evidence of secondary considerations should be afforded no weight. The Examiner's rejections based on obviousness were proper.

II. Conclusion

Therefore, it is requested that claims 1-60 all be finally rejected.

As identified in the attached Certificate of Service and in accordance with MPEP §2266.06 and 37 CFR §§1.248 and 1.903, a copy of the present response, in its entirety, is being served to the address of the attorney/agent of record at the address provided for in 37 CFR 1.33(c). Please direct all correspondence in this matter to the undersigned.

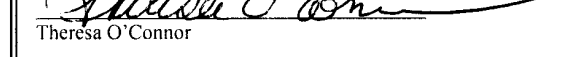
Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: June 29, 2012
HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: 214/651-5533
Attorney Docket No.: 43614.101

CERTIFICATE OF TRANSMISSION UNDER 37 CFR §1.8
I hereby certify that this correspondence and any corresponding filing fee is being transmitted via the Electronic Filing System (EFS) Web with the United States Patent and Trademark Office on June 29, 2012



Theresa O'Connor

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Larson et al.	§	*Inter Partes* Reexamination
	§	Control No. 95/001,851
U.S. Patent No. 7,418,504	§	
	§	Group Art Unit: 3992
Issued: August 26, 2008	§	
	§	Examiner: Roland Foster
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	§	Confirmation No.: 1688

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. §1.947 and Exhibits G-H, in their entirety, were served on:

McDermott Will & Emery
600 13th Street, NW
Washington DC 20005-3096

the attorney of record for the assignee of U.S. Patent No. 7,418,504, in accordance with 37 C.F.R. § 1.915 (b)(6), on June 29, 2012.

In addition, it is noted that the Patent Owner has requested that the Patent Office and Third Party Requester provide it with "double correspondence," in contravention of 37 U.S.C. § 1.33(c) and MPEP § 2622, by filing a Power of Attorney purportedly to change the attorney of record for this reexamination proceeding *only*. As the Patent Office has not yet rejected this request for double correspondence, a courtesy copy of the COMMENTS BY THIRD PARTY REQUESTER PURSUANT TO 37 C.F.R. §1.947 and Exhibits G-H in their entirety were served on:

Finnegan, Henderson, Farabow, Garrett & Dunner LLP
901 New York Avenue, NW
Washington DC 20001-4413

the attorneys identified in the Power of Attorney and who filed the Patent Owner's Response to Office Action, on June 29, 2012.

/David L. McCombs/

David L. McCombs, Registration No. 32,271

Exhibit G

Malkin, Gary, "Dial-in Virtual Private Networks Using Layer 3 Tunneling"

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

Dial-in Virtual Private Networks Using Layer 3 Tunneling

Gary Scott Malkin
Bay Networks
gmalkin@baynetworks.com

Abstract

Corporate Networks are making increasing use of the Internet to connect geographically diverse site networks rather than developing their own "leased line" WAN networks. Similarly, they are outsourcing their dial-in capability by replacing their banks of modems with a single connection to a Service Provider with geographically diverse Points Of Presence (POPs). In this way, users in a Corporate Network can dial local (or toll-free) numbers which will be routed to the nearest POP; then, be connected to their Corporate Network using some form of tunneling. There are two common forms of tunneling in use in the Internet today: Layer 2 (using L2TP, *for example) and Layer 3 (using* Mobile IP, *for example).*

This paper presents a design for a Layer 3 Dial-in Virtual Private Network Service (DVS), based on Mobile IP. *This design has been implemented by* Bay Networks.

1. Introduction

A Virtual Private Network is a network that uses a private IP address space (which may or may not be registered) that operates over another network's infrastructure. That is, the Virtual Private Network uses the same physical cabling, switches, bridges and routers, but uses a different address space. This is accomplished by encapsulating the Virtual Private Network traffic (which does not necessarily have to be IP traffic) in IP packets that use the physical infrastructure. There are two "standard" mechanisms that implement this encapsulation. The first is a Layer 2 (Datalink Layer) solution, such as L2TP [1] (a combination of Cisco's® L2F protocol and Microsoft's® PPTP protocol). The second is a Layer 3 (Network Layer) solution, such as Mobile IP [2] (developed within the IETF).

Consider the topology shown in figure 1. It illustrates a Service Provider's network that the Corporate Network uses for Dial-in Virtual Private Network service. A Layer 2 solution would establish a Point-to-Point Protocol (PPP) [3] connection between the Remote Node and the Customer Premise Equipment. This solution requires that the Remote Node and Customer Premise Equipment be L2TP aware. Further, the Customer Premise Equipment bears the entire burden of terminating the PPP connections; it is not simply a router.

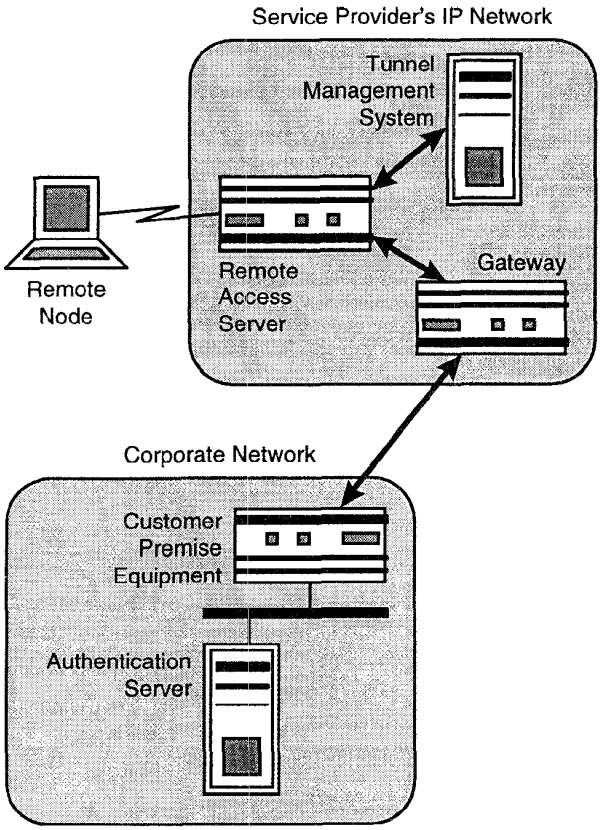


Figure 1. Topology

A Layer 3 solution terminates the PPP at the Remote Access Server, encapsulates (tunnels) the Remote Node's

traffic to the Gateway, and the Customer Premise Equipment *is* simply a router. This solution requires only an IP/PPP stack on the PC, several of which are readily available if not included in the Operating System, and places no load on the Customer Premise Equipment (beyond standard packet forwarding of the Remote Node's traffic).

2. Infrastructure Components

The physical infrastructure of the network shown in figure 1 consists of the following components:

- Remote Node
  This is the device with which the user accesses the Dial-in Virtual Private Network service. It is usually a PC, but could be a router with additional networks and nodes behind it.
- Remote Access Server
  This is the Public Switched Telephone Network's (PSTN) access into the Service Provider's network. It may handle Plain Old Telephone Service (POTS) or Integrated Service Digital Network (ISDN) traffic. There may be multiple Remote Access Servers in a POP. In the Layer 3 solution, this is the Mobile IP Foreign Agent.
- Tunnel Management System
  This is the host server that runs the Tunnel Management System software. It is essentially a database lookup engine that returns to the Remote Access Server the provisioned information necessary to authenticate a user and establish a path, which includes a tunnel, to that user's Corporate Network.
- Gateway
  This is the Corporate Networks' access into the Service Provider's network. It may handle any type(s) of "Virtual Circuit" connections into the Corporate Networks (e.g., dedicated serial line, Frame Relay, ATM). In the Layer 3 solution, this is the Mobile IP Home Agent.
- Customer Premise Equipment
  This is the Service Provider's access into the Corporate Network. In general, it has a static route for the subnet(s) that are used by Dial-in nodes. In the Layer 3 solution, this is a generic router.
- Authentication Server
  This is a host-based authentication server that communicates to the Remote Access Server, via the Gateway, using an authentication protocol (e.g., RADIUS [4]). Placing the Authentication Server in the Corporate Network allows the Corporate Network's administrator to manage that network's users without Service Provider intervention.

3. Operational Algorithm

Figure 2 shows the operational timeline for the lifetime of a Dial-in Virtual Private Network Service connection.

In step 1, the Remote Node dials in to the Remote Access Server. This may be a POTS or ISDN connection. It may have been a direct call to that POP or a call that has been directed to the POP by a rotary.

In the step 2, the Remote Node and the Remote Access Server complete PPP LCP negotiation. This is standard PPP. Multilink PPP [5] may also be used because the PPP fragments from the multiple dial-in lines are recombined by the bundle head at a Layer 2 and the tunnel exists at Layer 3.

In step 3, the Remote Node and the Remote Access Server begin PPP authentication. The PPP Packet Authentication Protocol (PAP) [6] may be used, but the Challenge Handshake Authentication Protocol (CHAP) [7] is recommended because it is more secure. Once the user has provided his/her userid and password, the standard authentication algorithm is interrupted and the tunnel creation algorithm begins. Authentication will be completed later. The reason for this is to prevent Network Control Protocols (NCPs) from beginning before the tunnel has been established. In this way, the Remote Access Server does not have to buffer packets from the Remote Node. Also, PPP clients are more temporally forgiving during the PPP authentication phase than during the NCP phase.

In step 4, the Remote Access Server sends the userid to the Tunnel Management System server. The Tunnel Management System must then decide whether the user should be authenticated, or whether a tunnel needs to be established to a Corporate Network. While the criteria used to make this determination can vary, the usual criterion is whether or not the userid is a Fully Qualified Domain Name (FQDN). In general, if the userid is an FQDN, then a tunnel is established to the Corporate Network identified by the domain portion of the userid; otherwise, the user is simply authenticated.

In step 5, the Tunnel Management System returns to the Remote Access Server all of the information necessary to complete authentication and establish the tunnel. This provisioned information is kept in a database on the Tunnel Management System server. At a minimum, the provisioned information includes the following (for each domain):

- Endpoint Identifier
  This is the IP address of the Gateway. In Mobile IP terms, this would be the Home Agent address.
- Authentication Server
  This is the IP address of the Authentication Server in the Corporate Network.

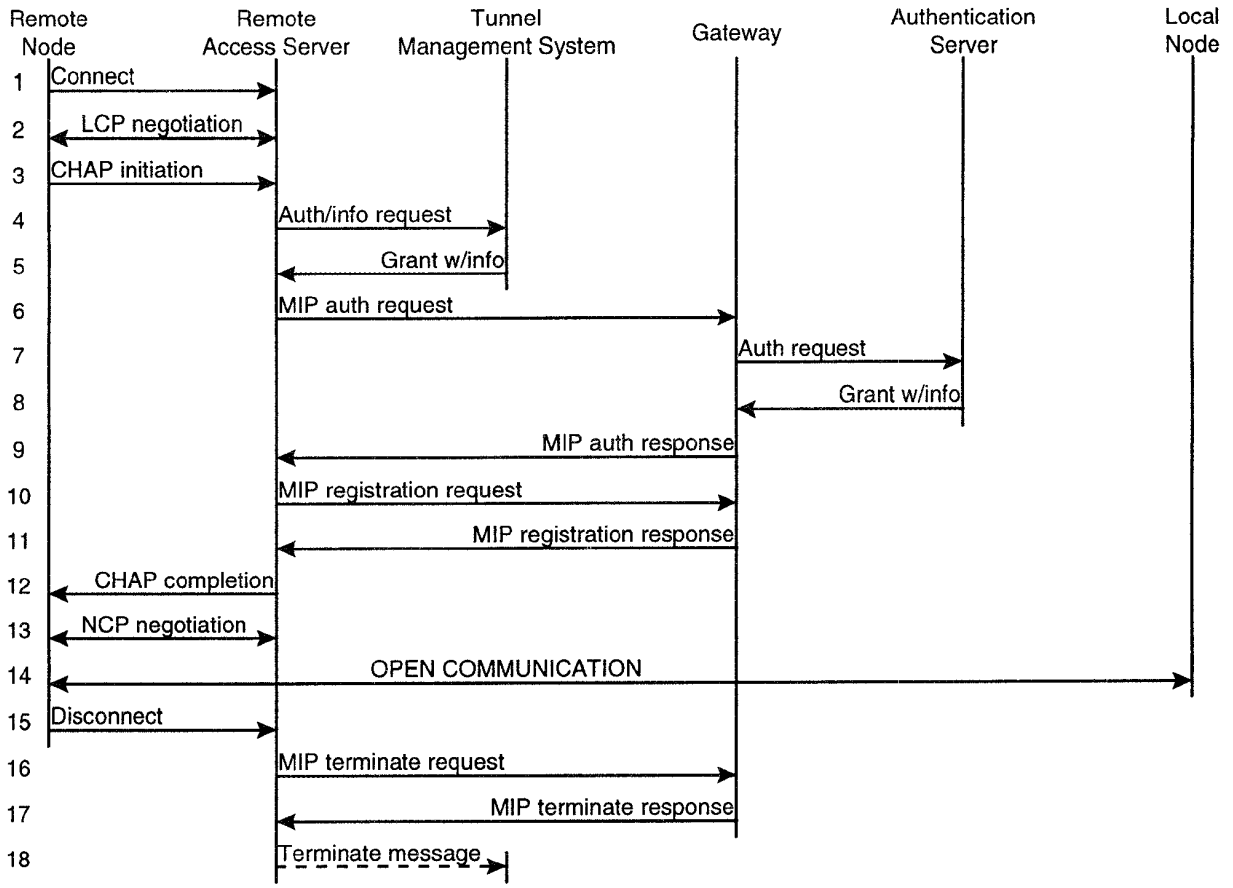


Figure 2. Operational Timeline

♦ Authentication Protocol

This is the protocol used by the Authentication Server (e.g., RADIUS).

Additional information could include accounting server address and protocol, tunnel authentication protocol and key, maximum number of users, and Gateway⇔Customer Premise Equipment connection hardware type (for some types (e.g., Frame Relay) an address (e.g., a DLCI) is required).

In step 6, the Remote Access Server sends a Mobile IP Authentication request (this is an extension to the Mobile IP protocol) to the Gateway, the address of which came from Tunnel Management System. The request contains all of the information the Gateway needs to contact the Authentication Server.

In step 7, the Gateway converts the Mobile IP Authentication request into the authentication protocol's authentication request and sends that to the Authentication Server. The authentication protocol (e.g., RADIUS) and the IP address of the Authentication Server are taken from the Mobile IP Authentication request sent by the Remote Access Server.

In step 8, the Authentication Server responds to the Gateway. The response will include an indication of whether or not the user is authenticated. If the user is granted access, the response will also contain the IP address that should be assigned to the Remote Node during the PPP Internet Protocol Control Protocol (IPCP) [8] negotiation. Other protocols (e.g., IPX, AppleTalk) may also be supported.

In step 9, the Gateway converts the authentication protocol's response into a Mobile IP Authentication response (also part of the extension to Mobile IP) and sends that to the Remote Access Server.

If the response is a "deny," the Remote Access Server terminates connection with the Remote Node.

In step 10, the Remote Node sends a Mobile IP Registration request to the Gateway. This serves to initiate tunnel establishment. The request may be authenticated (see section 6.3) using a cryptographic checksum or message digest (e.g., MD5 [9]). As a performance

enhancement, the tunnel identifier that the Remote Access Server supplies to the Gateway should be the physical port number to which the user is dialed-in. In this way, traffic from the Corporate Network to the Remote Node need not be routed; it may simply be forwarded directly to the port indicated by the tunnel identifier.

In step 11, the Gateway responds to the Mobile IP Registration request. As a performance enhancement, the tunnel identifier that the Gateway supplies to the Remote Access Server should be associated with the physical port that leads to the Customer Premise Equipment (e.g., a port number for a serial line or a DLCI for Frame Relay).

In step 12, the tunnel has been established. The Remote Node and the Remote Access Server now complete the PPP authentication phase.

In step 13, the Remote Node and the Remote Access Server now complete the PPP NCP phase. Any protocols for which the necessary NCP negotiation information was supplied in the Mobile Authentication response may be negotiated (e.g., IPCP, IPXCP, ATCP).

In step 14, the PPP connection has been established. Any packets sent by the Remote Node will now be tunneled through the Service Provider's network to the Gateway, then sent on to the Customer Premise Equipment, and finally routed to their destination in the Corporate Network. Similarly, packets from the Corporate Network are routed to the Customer Premise Equipment, which sends them on to the Gateway, which tunnels them through the Service Provider's network to the Remote Access Server, which sends them over the PPP connection to the Remote Node. See section 4 for details on packet encapsulation.

In step 15, the Remote Node disconnects from the Remote Access Server. It may be a graceful disconnection (i.e., the Remote Node may send a PPP termination request), or it may be a hang-up (i.e., the Remote Access Server loses Carrier Detect).

In step 16, the Remote Access Server sends a Mobile IP Termination Request to the Gateway to bring down the tunnel.

In step 17, the Gateway responds to the Mobile IP termination request. At this point the tunnel is closed.

Step 18 is an optional step. It occurs when the maximum users feature is implemented. See section 6.2 for details on the maximum users count.

4. Encapsulation

The path between the Remote Access Server and the Gateway is a Layer 3 (IP) tunnel. As shown in figure 3, packets generated by a Remote Node are received by the Remote Access Server which strips the PPP framing. The remainder of the packet (including the Layer 3 framing) is encapsulated using Generic Routing Encapsulation (GRE) [10]. The GRE framed packet is then framed as an IP datagram. The datagram is then Layer 2 framed for the output interface the Remote Access Server will use to reach first hop on the path to the Gateway (e.g., Ethernet). This datagram is forwarded through the Service Provider's network. When the Gateway receives a datagram whose protocol type is GRE, it will strip off the GRE header, remembering the tunnel identifier. Based on the tunnel identifier, the Gateway will determine the output interface it should use to reach the Customer Premise Equipment. It will frame the packet appropriately for the interface type and send the newly framed packet out on the interface. On reception, the Customer Premise Equipment will strip off the interface framing. At this point, the packet is the same packet the Remote Access Server received after striping off the PPP framing. The Customer Premise Equipment now routes this packet in the usual way.

5. Error Recovery

There are two general errors that may occur. The first is a failure of the Remote Access Server. If the port to which the user is connected should fail, the system will treat this as a disconnection by the Remote Node. This will cause a Mobile IP Termination to be sent to the Gateway, which will cause the tunnel to be taken down gracefully.

If the Remote Access Server fails completely (i.e., it crashes), the Gateway will detect this when the Remote Access Server fails to reregister its tunnels within the

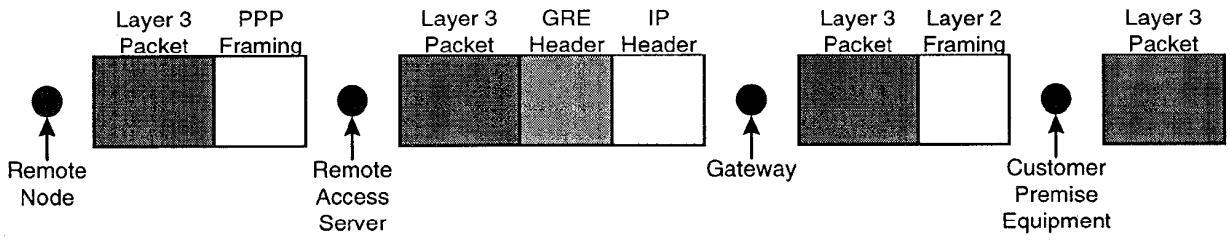


Figure 3. Encapsulation

time-out period. The Gateway will then take down the tunnels, as they time out. Any packet received for a tunnel that has been taken down will be dropped (an ICMP [11] may be generated).

If the Gateway fails, the Remote Access Server will detect this when the Gateway fails to respond to reregistration requests within the time-out period. The Remote Access Server will then take down the tunnels as they time out. When a tunnel is taken down, the connection to the Remote Node associated with that tunnel (as determined by the tunnel identifier, for example) will be dropped.

6. Enhancements

There are several enhancements to the system which may be implemented.

6.1. Called Number

Some PSTN systems (e.g., ISDN) provide the call recipient with the called number. This should not be confused with Caller ID, which is the call originator's number. Typically, the called number is presented to the modem prior to the assertion of Ring Indicate (i.e., before the phone "rings"). The called number (also referred to as a DNIS) may be used by the Tunnel Management System to determine the Corporate Network to which the user belongs. There are two basic ways in which it may be used to do this.

The first is to pass the called number to the Tunnel Management System server along with the userid (see figure 2, step 4). The Tunnel Management System then does a database lookup based on the userid and the called number. This is useful for very large Corporate Networks because they can load-share across multiple Gateways based on the called number. It is also useful for Corporate Networks that have geographically diverse sites, but share a common domain name. In practice, a lookup based on a domain/called number pair may be done in several ways. The first, and simplest, is to concatenate the two values to form a single database entry key. The disadvantage of this method is that the called number becomes a required value; users calling into a POP which does not support called number would need some form of domain-only lookup. This can be accomplished by creating a database entry whose key is the domain concatenated with "0." However, this eliminates the advantages of using the called number in first place. The other ways involve a primary/secondary lookup mechanism. This method would first search the database for the domain (or called number), then search the set of returned entries by called number (or domain). The disadvantage of this method is that the database engine must support reasonably complex search criteria.

The second way to use the called number is to create a Tunnel Management System that considers only the called number. This alters the basic connection/tunnel establishment algorithm, as defined in section 3. Rather than waiting for the Remote Node to provide the userid, the Remote Access Server could, on reception of the called number, immediately issue the auth/info request to the Tunnel Management System. By the time the Remote Node has provided the userid, the Remote Access Server should have received a response from the Tunnel Management System. Once the userid and Tunnel Management System response are both available, the Remote Access Server could then send the Mobile IP Authentication request to the Gateway. The disadvantage of using only the called number is that the Service Provider must provide a different phone number (or set of phone numbers) for each Corporate Network.

6.2. Maximum User Count

Limiting the number of concurrent users per-domain has two important uses. The first is the ability for the Service Provider to charge the Corporate Networks more for a larger number of concurrent users. The second is that the Service Provider can control the maximum offered load to network. The maximum offered load is a function of the sum of the maximum number of users for each domain, and the speed of the modems attached to the Remote Access Servers.

To implement a maximum users count, the Tunnel Management System database will contain a per-domain field which specifies the maximum number of users which may be active concurrently. The database will also contain state information; that is, it must keep track of the number of currently active users per-domain. When a request is received from a Remote Access Server, the Tunnel Management System will compare the current active users count to the maximum active users count. If the new user is not over the threshold, the provisioned information can be returned to the Remote Access Server; otherwise, a "deny" is returned.

Step 18 of figure 2 shows the Remote Access Server issuing a Terminate message to the Tunnel Management System. This is the message the Tunnel Management System uses to decrement the active user counts.

In Multilink PPP, each link is individually authenticated before being attached to the bundle head. This implies that each successive link will pass through the Tunnel Management System. It therefore follows that each link is counted as a user. Therefore, if the maximum number of users is 10, and five users each connect with

two links, a sixth user will not be able to connect. In a sense, this is what the Service Provider should want because multiple links consume more bandwidth which, after all, is what the Service Provider is charging for.

In order to recover from errors properly, the Tunnel Management System must keep track of the number of concurrent users, per domain, connected to each Remote Access Server. That is, the Tunnel Management System does not maintain a simple count of the total number of active users, but rather, remembers how many users on each Remote Access Server are connected to a given domain. This is done so that, if a Remote Access Server crashes, the Tunnel Management System can decrement the number of active users, for every domain, by the number of users tunneled to each domain from the Remote Access Server that crashed. If this is not done, then successive crashes could cause the active user count for a domain to grow until the maximum number of active users is reached, yet no users are actually connected. The mechanism by which the Tunnel Management System determines that a Remote Access Server has crashed is beyond the scope of this paper.

6.3. Registration Authentication

An important security consideration is the authentication of the Remote Access Server to the Gateway, and vice-versa, during tunnel registration. This can be accomplished by using a cryptographic checksum or message digest (e.g., MD5) on the Mobile IP Registration request and response packets. The key distribution mechanism is beyond the scope of this paper.

Note that full encryption of the packets is not required, only authentication. This is because the packets do not contain any sensitive information.

6.4. Accounting

There are two types of accounting to consider. The first is a simple count, maintained by the Tunnel Management System, of the number of grants and denies issued on a per-domain basis. This may be sufficient if the Service Provider charges a simple flat-rate based on the maximum number of active users. The second is a more comprehensive accounting system that tracks the number of packets, the number of octets, and the duration of each connection. These statistics are more easily gathered on the Gateway than on the Remote Access Server. The reason is that the Remote Node may be using Multilink PPP, and it would be difficult to combine the statistics from each of the ports. It is especially difficult for connections which come and go on a on-demand basis. Because the tunnel endpoint on the Gateway is a "choke-point" through which all traffic between the Remote Node and Corporate Network must pass, it is ideally situated to record these statistics.

It is also possible to incorporate an accounting protocol (e.g., RADIUS accounting [12]). The protocol type and accounting server address may be stored in the Tunnel Management System database and passed to the Gateway in the Mobile IP Authentication request.

6.5. Dynamic Remote Node Address Assignment

The system, as described so far, relies on the Authentication Server to provide a Layer 3 address, or addresses, to the Remote Node. In general, this results in the need to assign a unique address to every user. Because fewer users than the total number can access the system concurrently, this results in a waste of address space. This is particularly a problem in IP. There are two solutions to this problem.

In the first solution, the Authentication Server could do some form of dynamic address assignment. The problem with this solution is that an Authentication Server is typically stateless; therefore, it is unable to reap addresses as users disconnect from the system. There are ways around this problem if the Authentication Server is also the Accounting Server and can detect when a user disconnects.

In the second solution, the Gateway, on detecting that the Authentication Server did not supply a Layer 3 address, may do an address assignment request on behalf of the Remote Node. The addresses of the address allocation server would have been provided by the Tunnel Management System, via the Mobile IP Authentication request. Because the Gateway is directly attached to the Corporate Network, it can maintain leases on the assigned address. Because it knows when the user disconnects (it gets a Mobile IP Termination request), it can free the address immediately. The problem with this solution is that the only dynamic address assignment protocol is the Dynamic Host Configuration Protocol (DHCP) [13], and it only provides IP addresses.

6.6. Secondary Servers

The Tunnel Management System database may contain the addresses for secondary authentication, accounting and address assignment servers. The mechanism by which the system recognizes that the primary server(s) are down is beyond the scope of this paper.

7. Security Considerations

There are two forms of security to consider. The first is authentication between the Remote Access Server and the Gateway. This is highly recommended, as the creation of the tunnel is a vulnerable point in the establishment of the

path between the Remote Node and the Customer Premise Equipment.

The second form of security is encryption of the user's data as it travels between the Remote Access Server and the Gateway. This is not typically necessary because it does not offer much in the way of protection. An eavesdropper is much more likely to sniff the choke-points into (the PSTN) and out of (the Gateway⇔Customer Premise Equipment connection) the Service Provider rather than try to sort out packets within the Service Provider's network. Mobile IP does specify the use of IP Security (IPSEC), but that is still a work in progress contained in several Internet Drafts. The best way to ensure the privacy of data is to do end-to-end encryption. Not only does this leave no unencrypted point in the data path, but it distributes the load generated by the encryption algorithms.

8. Conclusion

This paper has presented the protocols and algorithms that may be used to implement a Layer 3 tunneling solution for Dial-in Virtual Private Networks. The question remains, "What are the advantages of a Layer 3 solution over a Layer 2 solution?"

The most important advantage, and the guiding principle behind most of the architecture, is that no special code is required on either the Remote Node or the Customer Premise Equipment. All the Remote Node needs is a standard IP/PPP stack; the Customer Premise Equipment can be from any vendor.

Other significant advantages to the Layer 3 solution includes:

- The Service Provider does not take part in the Corporate Network's routing. If the Remote Node is a router, and there are nodes and networks behind it, the routing packets between the Corporate Network and the Remote Router are handled just like any other data packet by the Service Provider's network.
- The Corporate Network does not require a globally unique (i.e., registered) address space because the addresses in the Corporate Network and the address of the Remote Node are hidden from the Service Provider's network, and from other Corporate Networks connected to the Service Provider.
- No additional load is placed on the Customer Premise Equipment. Because PPP and tunnel termination occurs on the Service Provider's equipment, the Customer Premise Equipment is simply a router.
- The scaling is better because the overhead of tunnel maintenance and packet encapsulation is distributed across the Service Provider's equipment. The Tunnel Management System need not reside on a single server; it can be based on a multi-node database engine.

None of these advantages negate the Layer 2 solution's usefulness in other applications. It may be used, for example, to carry Multilink PPP fragments between Remote Access Servers (Multi-node Multilink PPP).

9. References

[1] Hamzeh, K., T. Kolar, M. Littlewood, G. Pall, J. Taarud, "Layer Two Tunneling Protocol 'L2TP,'" IETF Work in Progress.

[2] Perkins, C., "IP Mobility Support," RFC 2002, October, 1996.

[3] Simpson, W., "The Point-to-Point Protocol (PPP)," RFC 1661, July, 1994.

[4] Willens, S., A. Rubens, W. Simpson, C. Rigney, "Remote Authentication Dial In User Service," RFC 2059, January, 1997.

[5] Sklower, K., B. Lloyd, G. McGregor, D. Carr, T. Coradetti, "The PPP Multilink Protocol (MP)," RFC 1990, August, 1996.

[6] Lloyd, B., W. Simpson, "PPP Authentication Protocols," October, 1992.

[7] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)," RFC 1994, August, 1996.

[8] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)," RFC 1332, May, 1992.

[9] Rivest, R., "The MD5 Message-Digest Algorithm," RFC 1321, April, 1992.

[10] Hanks, S., T. Li, D. Farinacci, P. Traina, "Generic Routing Encapsulation (GRE)," RFC 1701, October, 1994.

[11] Postel, J., "Internet Control Message Protocol," RFC 792, September, 1981.

[12] Rigney, C., "RADIUS Accounting," RFC 2059, January, 1997.

[13] Droms, R., "Dynamic Host Configuration Protocol," RFC 1541, October 1993.

Exhibit H

Ortiz Jr., Sixto, "Virtual Private Networks: Leveraging the Internet"

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

Virtual Private Networks: Leveraging the Internet

Sixto Ortiz Jr.

Proponents say virtual private networks could be the wave of the networking future for one very important reason: VPNs transmit data via the Internet, rather than via expensive traditional private networks.

Proponents are quick to mention the significant cost savings organizations can realize by using networks that employ the Internet backbone as a data pipeline rather than networks that rely on leased lines, frame-relay technology, and dial-up connections for private WANs.

However, as with many Internet technologies, potential VPN users are concerned about possible security, reliability, and performance problems. In addition, a lack of open standards has created concerns about compatibility. The industry is working toward adoption of such standards, but it remains to be seen whether this will lend credibility to VPN technology.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org

HOW A VPN WORKS

A VPN provides network-to-network or remote-user-to-network connectivity via an encrypted tunnel through the public Internet. Data must be encapsulated within an IP packet before it can be sent across a VPN. Network owners use various encryption and authentication schemes to provide security.

VPNs transmit encrypted data via the Internet, rather than via expensive traditional private networks.

To access a VPN, authorized users dial either a local ISP or a dedicated line to connect to the private network via the Internet.

Some VPNs require specialized hardware, while others may consist of specialized software that adds VPN capabilities to a firewall, server, or router.

For example, Raptor Systems (http://www.raptor.com) has developed firewalls with VPN capabilities. And IBM (http:// www.ibm.com) has developed routers that house VPN software and hardware that permit LAN-to-LAN connectivity.

Extended Systems' (http://www.extendedsystems.com) ExtendNet VPN server, shown in Figure 1, lets a remote user access a LAN via the Internet. The user must have the proper password to access the server, which is a separate node on the LAN. Once connected, remote clients running Windows 95 or Windows NT can send and receive data in the same way they would use a physical network connection. Remote users need specialized software to access VPNs.

To operate its own VPN, an organization needs a systems administrator with expertise in authentication, encryption, and other security issues. To avoid these complexities, some organizations are turning to ISPs—such as PSINet (http://www.psinet.com), Savvis Communications (http://www.savvis.com), and GTE Internetworking (http://www.bbn.com)—for the network infrastructure and expertise necessary to set up, run, and maintain their VPNs.

ISPs will become a critical driver of VPN technology, said Vaughn Harring, a spokesman for GTE Internetworking.

In fact, Michael Gaddis, Savvis Communications' executive vice president and chief technology officer, said he expects his company to receive an increasing amount of revenue from VPNs during the next few years.

However, if an ISP runs an organization's VPN, that network becomes dependent on the provider. If the ISP experiences bandwidth limitations or technical difficulties, the VPN will also experience problems.

ADVANTAGES

VPNs offer several advantages over traditional private networks. Barry Voltz, information systems manager with Omron Electronics, cites the significant cost savings provided by the company's VPN. Voltz also said the service has provided enhanced flexibility and convenience.

Cost savings

VPNs at least partially eliminate the modem banks, access servers, phone

lines, and other types of hardware organizations must install to provide remote access to traditional private networks.

In addition, VPNs can let remote users access networked resources via local telephone calls rather than, for example, via more expensive leased lines.

VPNs would be particularly cost-effective over longer distances, where leased lines are more expensive, and over multiple connections, where the additional cost of leased lines adds up, said John Pescatore, a consultant with Trusted Information Systems, a computer and communications security firm.

On the other hand, Pescatore noted, savings could be eroded because large VPN traffic volumes could cause processing bottlenecks as systems spend time encrypting and decrypting packets. To reduce these bottlenecks, users would have to buy more hardware.

Meanwhile, because VPNs are relatively new and involve complex security issues, it could be more expensive to hire a systems administrator for a virtual network than for a traditional network.

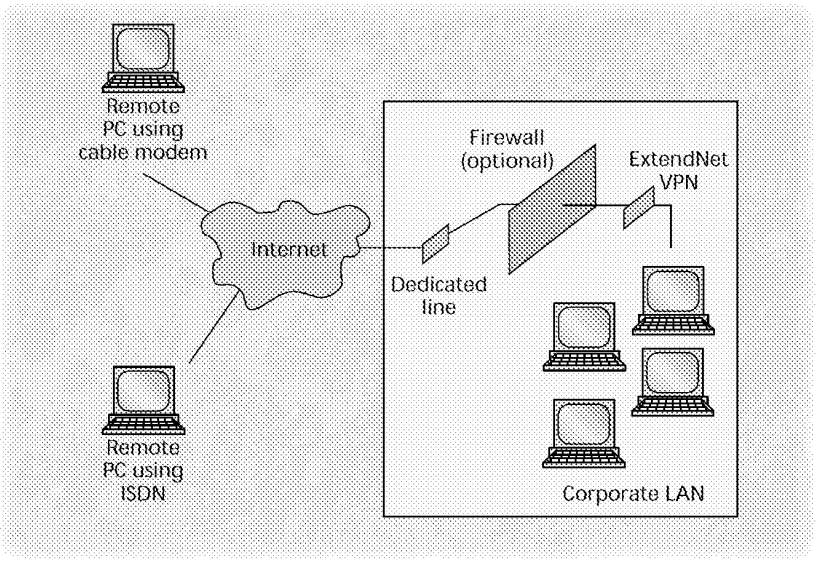


Figure 1. Extended Systems' ExtendNet VPN server is one way an organization can implement a virtual private network. A remote user can connect to the Internet via, for example, a cable modem or an ISDN line. The remote user then connects via the Internet backbone and a dedicated line to the VPN server. If authorized, the server will let the user connect to the organization's LAN.

Flexibility and convenience

VPNs can be more flexible and convenient than traditional networks in their ability to permit remote entry to any authorized user with Internet access.

VPNs also may eventually let business partners access networked resources via the Internet, thus providing the required backbone for strong business alliances. This can be difficult with traditional private networks, because organizations that want to share networked resources may have incompatible systems. This is a particular problem when many organizations, such as a large retailer and its suppliers, want to work together across a network.

DISADVANTAGES

VPNs face obstacles to widespread implementation, including questions about security, reliability, performance, and the lack of open standards.

Security

As with many Internet-related technologies, the security of communications and data transmission is an important issue for VPNs. Two key issues are user authentication, which can be accomplished with passwords, and the security of the VPN's encryption tunnel.

In addition, network managers must carefully manage VPN user-access policies, said Evan Kaplan, president of Aventail (http://www. aventail.com), a VPN software vendor.

As with many Internet-related technologies, the security of communications and data transmission is an important issue for VPNs.

These issues have caused some potential users to express concern that if their VPNs are run by ISPs, the level of security will be controlled by the service provider and may not be adequate.

VPN product vendors support a wide variety of encryption and authentication schemes to try to address these concerns.

For example, Aventail has a software product designed to provide client authentication and encryption at the session layer.

VPNet Technologies (http:// www. vpnet.com) has a hardware box that goes between the router and the WAN, to provide encryption, authentication, and compression.

Most vendors implement at least 56-bit encryption compliant with the Data Encryption Standard (DES), which is quite secure, according to Trusted Information Systems' Pescatore.

However, many experts and industry observers say 56-bit encryption is not strong enough. Some VPN vendors offer 112-bit DES encryption. However, increased encryption may degrade performance because stronger algorithms will divert processing power.

Reliability and performance

Because VPNs use the Internet, they can incur reliability and performance problems due to congestion, dropped packets, and other factors. This could cause problems for real-time applications, such as telephony and videoconferencing.

Some large ISPs are trying to alleviate reliability concerns by keeping all cus-

tomer VPN traffic on their own backbones. However, this won't always guarantee reliability because ISPs can experience problems on their backbones and cannot eliminate all problems associated with Internet transmissions.

Standards

The lack of open standards is a significant barrier to the widespread use of VPNs. Without standards, many users might not invest in VPN technology out of concern that they might buy products that could quickly become obsolete and unsupported, said Jim Balderstone, an analyst with Zona Research, a market research firm. In light of this, the industry is moving rapidly toward developing open standards.

The lack of open standards is a significant barrier to the widespread use of VPNs. Without standards, many users might not buy VPN technology.

For example, the IETF recently began considering the Layer 2 Tunneling protocol (L2TP), which combines Microsoft's Point-to-Point Tunneling protocol and Cisco Systems' Layer 2 Forwarding protocol. L2TP would permit users with protocol-compliant hardware and software from different vendors to work across the same VPN.

The IETF is also considering IPSec (IP Security protocol), a set of open standards for the authentication and encryption of IP packets. IPSec would beef up IP so that it provides the security requirements most organizations will demand before they send data across the Internet via a VPN.

Some industry observers contend that many organizations may decide not to use VPNs because of questions about security, reliability, and performance.

Nonetheless, Ray Keneipp, an analyst with Decisys, a network consulting firm, said he expects VPNs to become very popular in the near future, particularly for corporations with multiple branch offices, such as large insurance carriers. As the demand for bandwidth increases, such corporations simply won't be able to afford bandwidth-hungry applications if they have private lines, Keneipp said. ❖

Sixto Ortiz Jr. is a freelance writer and a part-time consultant with Currid and Company, a technology consulting firm. Contact him at sortiz@ tgn.net.

Electronic Acknowledgement Receipt

EFS ID:	13142587
Application Number:	95001851
International Application Number:	
Confirmation Number:	1688
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.101
Receipt Date:	29-JUN-2012
Filing Date:	13-DEC-2011
Time Stamp:	13:21:29
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Comments_by_Third_Party_Requester.pdf	2958264 298181cd11c7b18b4e4bcea06c6f51ed7d66d6d3	yes	55

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Third Party Requester Comments after Non-final Action	1	54
	Reexam Certificate of Service	55	55

Warnings:					
Information:					
2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_G_Malkin.pdf	2161427 18ee977b916de40b16c4086a6e7ce8e0d23287a7	no	8
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex_H_Ortiz.pdf	3634604 c463e9a6a2f3f200d256dc576278832bf2edc6da	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	8754295		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS

Date: 8-15-12

David L. McCombs
HAYNES AND BOONE, LLP, IP SECTION
2323 Victory Ave., Suite 700
Dallas, TX 75219

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001851
PATENT NO. : 7418504
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

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

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

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

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

PTOL-2070(Rev.07-04)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

MAILED

AUG 15 2012

CENTRAL REEXAMINATION UNIT

MCDERMOTT WILL & EMERY
600 13TH STREET, NW
WASHINGTON, DC 20005-3096

(For Patent Owner)

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

(For Third Party Requester)

Inter Partes Reexamination Proceeding
Control No. 95/001,851
Filed: December 13, 2011
For: U.S. Patent No. 7,418,504

DECISION GRANTING PETITION UNDER 37 CFR 1.183

This is a decision on the patent owner petition paper entitled "PETITION SEEKING WAIVER OF 37 C.F.R. § 1.943 FOR PATENT OWNER'S RESPONSE TO OFFICE ACTION OF MARCH 1, 2012" (the petition under 37 CFR 1.183), filed on June 1, 2012.

The petition under 37 CFR 1.183 is before the Office of Patent Legal Administration.

The petition under 37 CFR 1.183 is **granted** to the extent set forth below.

RELEVANT BACKGROUND

1. On August 26, 2008, U.S. patent number 7,418,504 (the '504 patent) issued to Larson *et al.*

2. On December 13, 2011, a third party requester filed a request for *inter partes* reexamination of the '504 patent, which request was assigned Reexamination Control No. 95/001,851 (the '1851 proceeding).

3. On March 1, 2012, the Office issued an order granting *inter partes* reexamination in the '1851 proceeding, concurrently with a non-final Office action.

4. On June 1, 2012, patent owner filed a response to the March 1, 2012 Office action, concurrently with the instant petition under 37 CFR 1.183.[1]

[1] On March 23, 2012, the Office mailed a decision granting a one-month extension of time for patent owner's response to the March 1, 2012 Office Action.

5. On June 29, 2012, requester filed a comments submission after the March 1, 2012 Office action and patent owner's June 1, 2012 response submission.

DECISION

I. Relevant Statutes, Regulations and Procedures

37 CFR 1.183 provides:

> In an extraordinary situation, when justice requires, any requirement of the regulations in this part which is not a requirement of the statutes may be suspended or waived by the Director or the Director's designee, *sua sponte*, or on petition of the interested party, subject to such other requirements as may be imposed. Any petition under this section must be accompanied by the petition fee set forth in § 1.17(f).

37 CFR 1.943(b) provides:

> Responses by the patent owner and written comments by the third party requester shall not exceed 50 pages in length, excluding amendments, appendices of claims, and reference materials such as prior art references.

II. Discussion

37 CFR 1.183 provides for suspension or waiver of any requirement of the regulations which is not a requirement of the statutes in an extraordinary situation, when justice requires, on petition of the interested party. The burden is on petitioner to set forth with specificity the facts that give rise to an extraordinary situation in which justice requires suspension of a rule. A showing which petitioner can make in support of a request for waiver of the 50-page limit of 37 CFR 1.943(b) can be an attempt to draft a patent owner's response or third party requester comments submission in compliance with the 50-page limit, and submission of a resulting response or comments submission that is in excess of 50 pages concurrently with a petition under 37 CFR 1.183 for waiver of 37 CFR 1.943(b), requesting entry of the proposed submission. Such a response or comments submission can be evaluated for economizing, extraneous material, and arrangement, without repetition of information already of record. In this way, petitioner can rely on the proposed response or comments submission: (1) for justification that more pages are needed to complete the response, and (2) to set forth an accurate determination of exactly how many additional pages petitioner deems to be needed for the response or comments submission.

It is noted that, for purposes of making an accurate determination of exactly how many additional pages over 50 are deemed to be needed for the response, a document is deemed to be subject to the 50-page length requirement when the document includes legal argument, *i.e.*, arguments of counsel such as, *e.g.*, arguments that the claims are patentable or unpatentable, or that are directed to how an outstanding or proposed rejection is overcome, or, in the case of a document filed by the requester, how an outstanding or proposed rejection is supported. Each determination of whether a document, such as an affidavit or declaration, contains information that will cause the document to be subject to the page count is made on a case-by-case basis. In determining whether a document such as an

affidavit or declaration under 37 CFR 1.132, or any other document of a submission, includes legal argument, the Office analyzes whether the document is providing factual evidence, *i.e.*, evidence of **technological facts,** or whether the document contains argument that is merely an extension of the arguments of counsel. Factual evidence includes, for example, declarations that swear behind the filing date of a reference, that establish the date of a printed publication, that provide a technical explanation or technical definition of terms of art used by a reference, or that provide comparative test results and a scientific, or technological, analysis of the results (*see, e.g.*, MPEP 716.02). If a document is limited to factual evidence, the document is not included in the page count. In addition, affidavits or declarations limited to establishing commercial success, long-felt need and failure of others, scepticism of experts, or copying, as per MPEP 716.03-716.06, respectively, will not be included in the page count.

III. Patent owner petition of June 1, 2012

On June 1, 2012, patent owner filed the instant petition under 37 CFR 1.183, requesting waiver of 37 CFR 1.943(b) to permit entry of its concurrently-filed response submission. Patent owner asserts that the June 1, 2012 response submission is 71 pages long, excluding amendments, appendices of claims, and reference materials.[2] Patent owner states that it also submitted two declarations, one by one of the inventors (Dr. Short) and another by an expert (Dr. Keromytis), but asserts that "[t]he declaration of Dr. Short presents facts regarding secondary considerations and the declaration of Dr. Keromytis discusses how one of ordinary skill in the art would have understood the references cited in the Office Action."[3] Patent owner asserts that it believes neither declaration should count towards the page limit.[4] Nonetheless, patent owner requests waiver of the 50-page limit to submit these declarations with its response "should the Office decide to include portions of either declaration in the page count for the response."[5]

In support of its request for waiver of the rule, patent owner asserts that the Office action adopted twenty-one grounds of rejection and "the Examiner incorporated by reference corresponding portions of the 39 pages of Cisco's request and 328 pages of accompanying claim charts."[6] Patent owner asserts that it "has made every effort to pare down its response," but that "limiting its response to 50 pages would severely compromise its ability to fully address the issues raised in the Office Action."[7] Patent owner further asserts that "even if the Office were to count the declarations towards the page limit, the total number of pages representing the response and the declarations would still be substantially less than the 39 pages of Cisco's request and 328 pages of accompanying claim charts relied upon and incorporated by reference in the Office Action."[8]

Based on the specific facts set forth in patent owner's petition under 37 CFR 1.183, patent owner's showing in support of the request for waiver of the 50-page limit of 37 CFR 1.943(b) by attempting to draft a response in compliance with the 50-page limit and submitting the resulting response

[2] Patent owner petition under 37 CFR 1.183 at page 1.
[3] Id. at page 3.
[4] Id.
[5] Id.
[6] Id. at pages 1-2.
[7] Id. at page 2.
[8] Id. at page 3.

(which is in excess of 50 pages),[9] and the individual facts and circumstances of this case (such as the length of the March 1, 2012 Office action),[10] it is deemed equitable to waive the 50-page limit of 37 CFR 1.943(b) in this instance. Accordingly, patent owner's petition under 37 CFR 1.183 is granted and the page limit of 37 CFR 1.943(b) is waived to the extent necessary to permit entry of patent owner's June 1, 2012 response submission. This waiver makes patent owner's June 1, 2012 response submission page-length compliant.

PATENT OWNER'S ADDRESS

Different patent owner addresses are of record for the patent and the reexamination proceeding. On February 6, 2012, patent owner filed a "REVOCATION OF POWER OF ATTORNEY, STATEMENT UNDER 37 C.F.R. § 3.73(b), AND GRANT OF NEW POWER OF ATTORNEY FOR REEXAMINATION CONTROL NO. 95/001,851 ONLY" in the '1851 proceeding. The paper requested that the address associated with Customer No. 22852 be recognized as the correspondence address for the '1851 proceeding.

Patent owner's February 6, 2012 paper was not effective to change the correspondence address of record for the '1851 proceeding. See *Revisions and Technical Corrections Affecting Requirements for Ex Parte and Inter Partes Reexamination*, 72 Fed. Reg. 18892 (April 16, 2007) (final rule) (stating, "The correspondence address for any pending reexamination proceeding not having the same correspondence address as that of the patent is, by way of this revision to § 1.33(c), automatically changed to that of the patent file..."). The current correspondence address of record for the patent file is the proper patent owner address for reexamination mailings pursuant to 37 CFR 1.33(c), and it is that of McDermott Will & Emery, 600 13th Street, NW, Washington, DC 20005-3096.

Accordingly, all future correspondence will be directed to, and service on patent owner should also be directed to, McDermott Will & Emery, 600 13th Street, NW, Washington, DC 20005-309. A courtesy copy of the instant decision is being provided to the address specified in patent owner's February 6, 2012 paper.

CONCLUSION

1. Patent owner's June 1, 2012 petition under 37 CFR 1.183 is **granted** and the 50-page limit of 37 CFR 1.943(b) is waived to the extent necessary to permit entry of patent owner's June 1,

[9] 71 pages of the remarks portion of patent owner's June 1, 2012 response submission count toward the regulatory page limit (the cover page and pages of the table of contents are excluded from the page count). Thus, the patent owner's June 1, 2012 response submission exceeds the 50-page limit by at least 21 pages, without including any portions of the 7-page Short declaration and 38-page Keromytis declaration that also count toward the regulatory page limit.

[10] On its face, the substantive portion of the March 1, 2012 Office action spans only approximately 20 pages, but in setting forth the rejections that have been adopted, it incorporates by reference approximately 350 pages from the '1851 request for *inter partes* reexamination, exceeding the number of pages of patent owner's proposed response, including any pages of the accompanying declarations that also count toward the regulatory page limit.

2012 response submission. This waiver makes patent owner's June 1, 2012 response submission page-length compliant.

2. Any questions concerning this communication should be directed to Maria Nuzzolillo, Legal Advisor, at (571) 272-8150 or Nicole D. Haines, Legal Advisor, at (571) 272-7717.

Pinchus M. Laufer
Senior Legal Advisor
Office of Patent Legal Administration

08-14-2012

cc: Finnegan, Henderson, Farabow, Garrett & Dunner LLP
901 New York Avenue, NW
Washington, DC 20001-4413

Re_Exam

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,851
U.S. Patent No. 7,418,504	Group Art Unit: 3992
Issued: August 26, 2008	Examiner: Roland Foster
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	Confirmation No.: 1688

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§ 1.933 AND 1.555

Pursuant to 37 C.F.R. §§ 1.933 and 1.555, VirnetX Inc., the patent owner, brings to the attention of the Examiner the documents listed on the attached PTO/SB/08 Form.

Copies of the listed non-patent literature documents are attached.

The patent owner respectfully requests that the Examiner consider the listed documents and indicate that they were considered by making appropriate notations on the attached form and returning the same to patent owner.

This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art." If the Examiner applies any of the documents as prior art against any claim in the instant proceeding and the patent owner determines that the cited documents do not constitute "prior art" under United States law, the patent owner reserves the right to present to

the U.S. Patent and Trademark Office the relevant facts and law regarding the appropriate status of such documents.

The patent owner further reserves the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims in the instant proceeding.

If there is any fee due in connection with the filing of this paper, please charge the fee to Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 20, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

IDS Form PTO/SB/08: Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 5

Complete if Known	
Control Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland Foster
Attorney Docket Number	11798.0007

U.S. PATENTS AND PUBLISHED U.S. PATENT APPLICATIONS

Tab No.	Examiner Initials*	Cite No.	Document Number Number-Kind Code *(if known)*	Issue or Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

Note: Submission of copies of U.S. Patents and published U.S. Patent Applications is not required.

FOREIGN PATENT DOCUMENTS

Tab	Examiner Initials*	Cite No.	Foreign Patent Document Country Code Number Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Translation

NON-PATENT LITERATURE DOCUMENTS

EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1119	Transcript of Hopen Deposition dated April 11, 2012 (57 pages)	
	D1120	Claim Construction Memorandum Opinion and Order in Case No. 6:10-CV-417 (31 pages)	
	D1121	Declaration of Angelos D. Keromytic, Ph.D. in Control No. 95/001,682 (98 pages)	
	D1122	Declaration of Dr. Robert Dunham Short III in Control Nos. 95/001,679; 95/001,682 (6 pages)	
	D1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.) (2 pages)	
	D1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. in Control No. 95/001,269 (9 pages)	
	D1125	Exhibit A-4, Redacted Deposition of Chris Hopen from VirnetX, Inc. v. Cisco Systems, Inc., No. 6:07-CV 417 (E.D. Tex. April 11, 2012 (5 pages)	
	D1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999 (23 pages)	
	D1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects (95 pages)	
	D1128	Exhibit B-3, Maryann Lawlor, Transient Partnerships Stretch Security Policy Management, Signal Magazine (Sept. 2001) http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes (5 pages)	
	D1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html. (5 pages)	
	D1130	Time Greene, CEO's Chew the VPN Fat, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch (6 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
				Control Number	95/001,851
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Filing Date	December 13, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Roland Foster
Sheet	2	of	5	Attorney Docket Number	11798.0007

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1131	Peter Alexander Invalidity Report in Case No. 6:10-cv-000417 (220 pages)	
	D1132	Defendants' Second Supplemental Joint Invalidity Contentions in Case No. 6:10-cv-0417 (3 pages)	
	D1133	Exhibit 118A, Altiga VPN System vs. Claims of the '135 Patent (251 pages)	
	D1134	Exhibit 119A, Altiga VPN System vs. Claims of the '151 Patent (73 pages)	
	D1135	Exhibit 120A, Altiga VPN System vs. Claims of the '180 Patent (78 pages)	
	D1136	Exhibit 121A, Altiga VPN System vs. Claims of the '211 Patent (95 pages)	
	D1137	Exhibit 122A, Altiga VPN System vs. Claims of the '504 Patent (95 pages)	
	D1138	Exhibit 123A, Altiga VPN System vs. Claims of the '759 Patent (123 pages)	
	D1139	Exhibit 12A, SSL 3.0 vs. Claims of the '135 Patent (25 pages)	
	D1140	Exhibit 13A, SSL 3.0 vs. Claims of the '504 Patent (33 pages)	
	D1141	Exhibit 14A, SSL 3.0 vs. Claims of the '211 Patent (33 pages)	
	D1142	Exhibit 228A, Understanding OSF DCE 1. for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '135 Patent (21 pages)	
	D1143	Exhibit 229A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '151 Patent (15 pages)	
	D1144	Exhibit 230A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '180 Patent (25 pages)	
	D1145	Exhibit 231A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '211 Patent[2]	
	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '504 Patent (44 pages)	
	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '759 Patent (28 pages)	
	D1148	Exhibit 255, Schulzrinne vs. Claims of the '135 Patent (28 pages)	
	D1149	Exhibit 256, Schulzrinne vs. Claims of the '504 Patent (122 pages)	
	D1150	Exhibit 257, Schulzrinne vs. Claims of the '211 Patent (122 pages)	
	D1151	Exhibit 258, Schulzrinne vs. Claims of the '151 Patent (49 pages)	
	D1152	Exhibit 259, Schulzrinne vs. Claims of the '180 Patent (41 pages)	
	D1153	Exhibit 260, Schulzrinne vs. Claims of the '759 Patent (74 Pages)	
	D1154	Exhibit 261, SSL 3.0 vs. Claims of the '151 Patent (14 pages)	
	D1155	Exhibit 262, SSL 3.0 vs. Claims of the '759 Patent (24 pages)	
	D1156	Exhibit 263, Wang vs. Claims of the '135 Patent (59 pages)	
	D1157	Wang vs. Claims of the '504 Patent (55 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Control Number	95/001,851
				Filing Date	December 13, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Roland Foster
Sheet	3	of	5	Attorney Docket Number	11798.0007

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1158	Wang vs. Claims of the '211 Patent (56 pages)	
	D1159	Exhibit 1, Alexander CV (22 pages)	
	D1160	Exhibit 2, Materials Considered by Peter Alexander (16 pages)	
	D1161	Exhibit 3, Cross Reference Chart (24 pages)	
	D1162	Exhibit 4, RFC 2543 vs. Claims of the '135 Patent (43 pages)	
	D1163	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent (46 pages)	
	D1164	Exhibit 6, RFC 2543 vs. Claims of the '211 Patent (46 pages)	
	D1165	Exhibit 7, The Schulzrinne Presentation vs. Claims of the '135 Patent (32 pages)	
	D1166	Exhibit 8, The Schulzrinne Presentation vs. Claims of the '504 Patent (36 pages)	
	D1167	Exhibit 9, The Schulzrinne Presentation vs. Claims of the '211 Patent (36 pages)	
	D1168	Exhibit 10, The Schulzrinne Presentation vs. Claims of the '151 Patent (15 pages)	
	D1169	Exhibit 11, The Schulzrinne Presentation vs. Claims of the '180 Patent (11 pages)	
	D1170	Exhibit 12, The Schulzrinne Presentation vs. Claims of the '759 Patent (29 pages)	
	D1171	Exhibit 13, SSL 3.0 vs. Claims of the '135 Patent (33 pages)	
	D1172	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent (38 pages)	
	D1173	Exhibit 15, SSL 3.0 vs. Claims of the '211 Patent (39 pages)	
	D1174	Exhibit 16, SSL 3.0 vs. Claims of the '151 Patent (10 pages)	
	D1175	Exhibit 17, SSL 3.0 vs. Claims of the '759 Patent (25 pages)	
	D1176	Exhibit 18, Kiuchi vs. Claims of the '135 Patent (30 pages)	
	D1177	Exhibit 19, Kiuchi vs. Claims of the '504 Patent (35 pages)	
	D1178	Exhibit 20, Kiuchi vs. Claims of the '211 Patent (35 pages)	
	D1179	Exhibit 21, Kiuchi vs. Claims of the '151 Patent (8 pages)	
	D1180	Exhibit 22, Kiuchi vs. Claims of the '180 Patent (19 pages)	
	D1181	Exhibit 23, Kiuchi vs. Claims of the '759 Patent (25 pages)	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401 vs. Claims of the '135 Patent (51 pages)	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '504 Patent (45 pages)	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '211 Patent (45 pages)	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401^2 vs. Claims of the '151 Patent (18 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Control Number	95/001,851
				Filing Date	December 13, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				Examiner Name	Roland Foster
Sheet	4	of	5	Attorney Docket Number	11798.0007

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1186	Exhibit 28 (2 pages)	
	D1187	Exhibit 29, The Altiga System vs. Claims of the '135 Patent (35 pages)	
	D1188	Exhibit 30, The Altiga System vs. Claims of the '504 Patent (40 pages)	
	D1189	Exhibit 31, The Altiga System vs. Claims of the '211 Patent (41 pages)	
	D1190	Exhibit 32, The Altiga System vs. Claims of the '759 Patent (35 pages)	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '135 Patent (64 pages)	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '504 Patent (39 pages)	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '211 Patent (41 pages)	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '151 Patent (19 pages)	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser") and RFC 2401 vs. Claims of the '180 Patent (33 pages)	
	D1196	Exhibit 38, Kent vs. Claims of the '759 Patent (17 pages)	
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent (48 pages)	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent (48 pages)	
	D1199	Exhibit 41, Aziz ('646) vs. Claims of the '759 Patent (24 pages)	
	D1200	Exhibit 42, The PIX Firewall vs. Claims of the '759 Patent (24 pages)	
	D1201	Exhibit A-1, Kiuchi vs. Claims of the '135 Patent (181 pages)	
	D1202	Exhibit B-1, Kiuchi vs. Claims of the '211 Patent (200 pages)	
	D1203	Exhibit C-1, Kiuchi vs. Claims of the '504 Patent (278 pages)	
	D1204	Exhibit D, Materials Considered (3 pages)	
	D1205	Exhibit E, CV of Stuart G. Stubblebine, Ph.D (19 pages)	
	D1206	Exhibit F, Claim Construction Chart (7 pages)	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents (60 pages)	
	D1208	Cisco Comments and Petition for Reexamination in Control No. 95/001,679 dated June 14, 2012 (69 pages)	
	D1209	Exhibit S, Declaration of Nathaniel Polish, Ph.D in Control No. 95/001,679 (5 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

IDS Form PTO/SB/08: Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				*Control Number*	95/001,851
				Filing Date	December 13, 2011
				First Named Inventor	Victor Larson
				Art Unit	3992
(Use as many sheets as necessary)				*Examiner Name*	Roland Foster
Sheet	5	of	5	*Attorney Docket Number*	11798.0007

NON-PATENT LITERATURE DOCUMENTS			
EXAMINER INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	TRANSLATION
	D1210	Exhibit R, Excerpts from Patent Owner & Plaintiff VirnetX Inc. 's First Amended P.R. 3-1 and 3-2 Disclosure of Asserted Claims and Infringement Contentions (53 pages)	
	D1211	Third Party Requester Comments dated June 25, 2012 - After Non Final Office Action in Control No. 95/001,788 (37 pages)	
	D1212	Reexam Affidavit/Declaration/Exhibit Filed by 3rd Party on June 25, 2012 in Control No. 95/001,788 (19 pages)	
	D1213	Extended European Search Report dated 03/26/12 from Corresponding European Application Number 11005793.2 (077580-0144) (6 pages)	
	D1214	Bergadano, et al., "Secure WWW Transactions Using Standard HTTP and Java Applets," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998 (12 pages)	
	D1215	Alexander Invalidity Expert Report dated May 22, 2012 with Exhibits (1542 pages)	
	D1216	Transcript of Deposition of Peter Alexander dated July 27, 2012 (55 pages)	
	D1217	Cisco '151 Comments by Third Party Requester dated August 17, 2012 with Exhibits (211 pages)	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dated August 17, 2012 (4 pages)	
	D1219	Transcript of August 22, 2012 Deposition of Stuart Stubblebine (69 pages)	

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,851
U.S. Patent No. 7,418,504	Group Art Unit: 3992
Issued: August 26, 2008	Examiner: Roland Foster
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	Confirmation No.: 1688

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

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.550 and M.P.E.P. § 2266.03, the undersigned attorney for the patent owner certifies that a copy of the Information Disclosure Statement, PTO Form SB/08, and listed references D1119-D1219 was served by first-class mail on September 20, 2012, on counsel for the third party requester at the following address:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219-7672

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 20, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,851	12/13/2011	7418504	43614.101	1688

22852 7590 10/01/2012

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

EXAMINER	
FOSTER, ROLAND G	
ART UNIT	**PAPER NUMBER**
3992	

MAIL DATE	DELIVERY MODE
10/01/2012	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

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

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

REEXAMINATION CONTROL NUMBER *95/001,851*.

PATENT NUMBER *7,418,504*.

TECHNOLOGY CENTER *3900*.

ART UNIT *3992*.

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

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

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

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

ACTION CLOSING PROSECUTION (37 CFR 1.949)	Control No.	Patent Under Reexamination
	95/001,851	7418504
	Examiner	Art Unit
	ROLAND FOSTER	3992

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

Responsive to the communication(s) filed by:
Patent Owner on 01 June, 2012
Third Party(ies) on 29 June, 2012

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

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

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

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

PART II. SUMMARY OF ACTION:

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

ACTION CLOSING PROSECUTION

1. Introduction

This Office action addresses claims 1-60 of United States Patent No. 7,418,504 B2 (the "Larson" patent), for reexamination was granted in the Order Granting *Inter Partes* Reexamination (hereafter the "Order"), mailed March 1, 2012.

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

The patent owner responded by filing arguments and associated evidence on June 1, 2012 (the "Response").

The third party requester responded by filing Comments to the Patent Owner's Response on June 29, 2012 (the "Comments").

The examiner has carefully considered the arguments and evidence provided in both the patent owner's Response and in the third party requester's Comments. Based on consideration of the entire record, the rejection of claims 1-60 is maintained. See the "Response to Arguments" section for further explanation. Accordingly, this Office action is made an "**Action Closing Prosecution**." See 37 CFR 1.949, MPEP 2671.02. See also the "conclusion" section to this Office action.

2. Prior Art Rejections

2.A. Issues Raised in the Request

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

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

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

Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP-The Development of a Secure, Closed HTTP-based Network on the Internet," Proceedings of the Symposium on Network and Distributed System Security, 1996 ("**Kiuchi**"), attached as Exhibit D-16 to the Request.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Claim Rejections - 35 USC § 102

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

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

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

Claim Rejections - 35 USC § 103

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

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

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

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

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

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

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

Summary

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

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

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

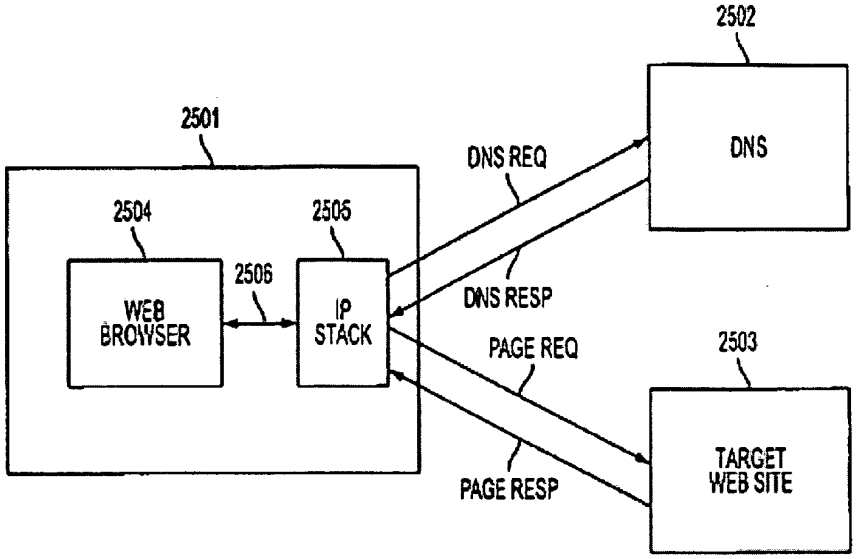


FIG. 25
(PRIOR ART)

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

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

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

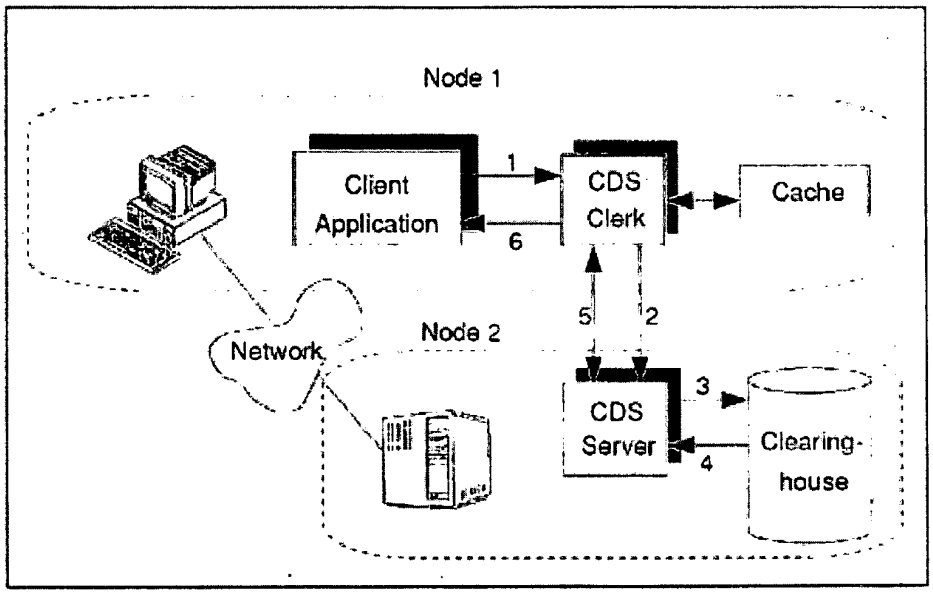


Figure 15. CDS Components Performing a CDS Look-up

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

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

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

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

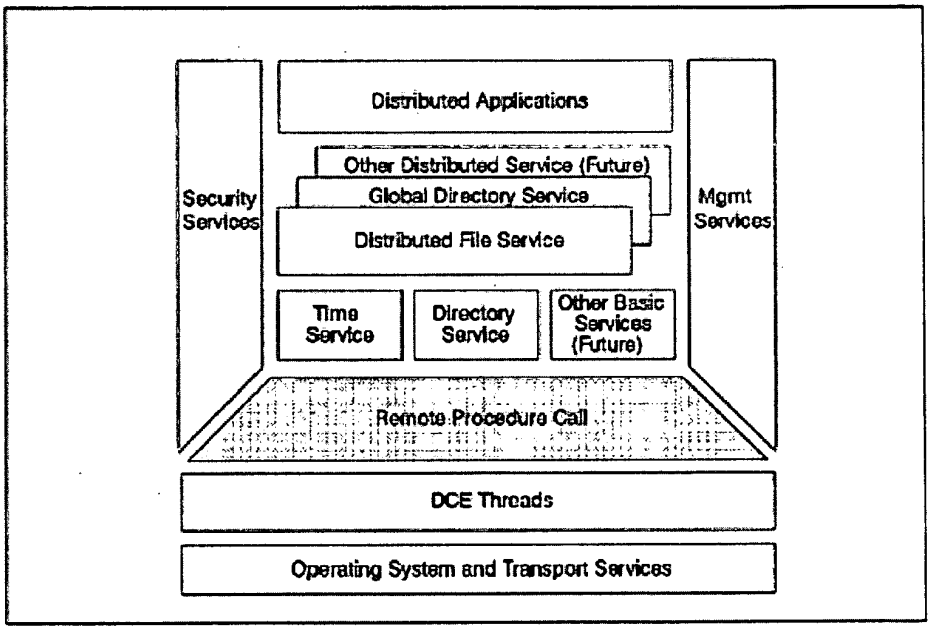


Figure 62. RPC as a DCE Component

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

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

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

Incorporation by Reference

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

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

Claim Rejections - 35 USC § 102

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

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

Claim Rejections - 35 USC § 103

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

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

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

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

Summary

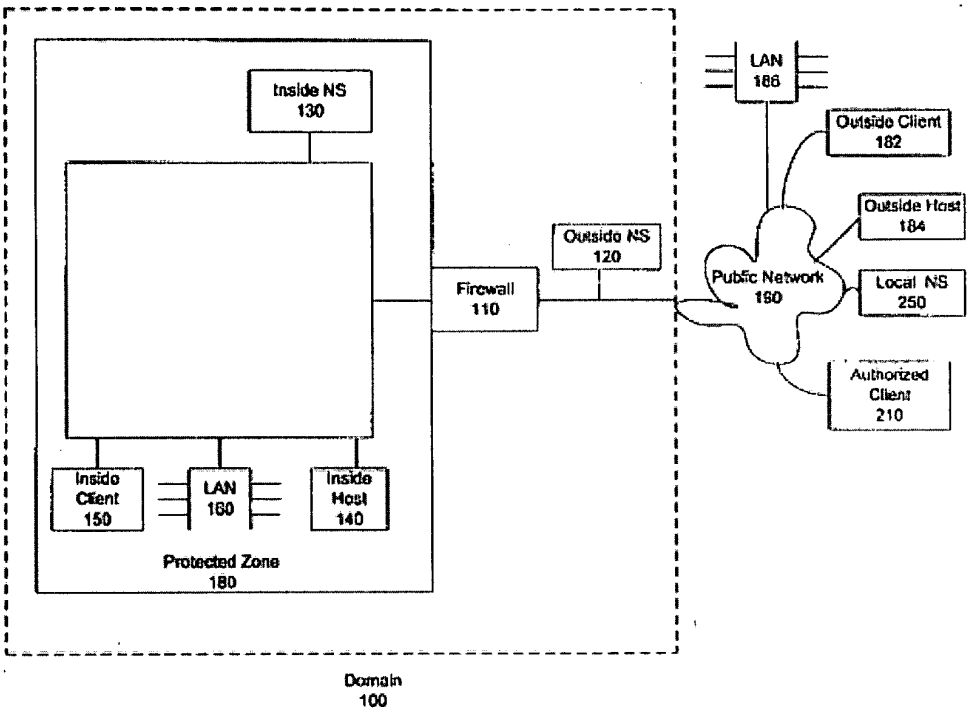
Independent claim 1 is representative of all independent claims, as discussed above. Similarly, the features of independent claim 1 have been discussed.

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

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

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

Fig. 1



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

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

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

> The registered name server for a domain is configured to return a new resource record type, herein called an SX record, in response to requests for information needed for secure communications with protected hosts in that domain. The resolver on (or otherwise associated with) the authorized client is configured to use the data in the SX record to dynamically update the information used by the client to handle secure communications.
>
> Col. 4, ll. 8-16.
>
> Alternatively, a name server can be configured to return an SX record in the response that includes the answer to a query for some other record. For example, if the client queries for a host address, a name server might send a response with the host address in the answer section and the SX record in the additional section.
>
> Col. 4, ll. 44-49.

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

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

Incorporation by Reference

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

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

Claim Rejections - 35 USC § 103

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

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

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

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

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

Summary

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

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

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

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

> A client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the name server confirms that the query is legitimate, it examines

> whether the requested server-side proxy is registered in the closed network and is permitted to accept the connection form the client-side proxy. If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values. If it is not permitted, it sends a status code which indicates an error...When the C-HTTP name server confirms that the specified server-side proxy is an appropriate closed network member, a client side proxy sends a request for connection to the server-side proxy, which is encrypted using the server-side proxy's public key....

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

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

Incorporation by Reference

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

3. Response to Arguments

3.1. Claim Interpretation

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

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

Thus, claim 1 recites a domain name service ("DNS") "system" and not a particular computer device or structural configuration, such as a single secure DNS server. Such an interpretation is consistent with the specification of the patent under reexamination, *see, e.g.*, col. 40, ll. 35-48, where the DNS system is implemented using gatekeeper 2603, DNS proxy 2610 and DNS server 2609. Thus, the DNS system can be distributed across multiple computer systems. Accordingly, the DNS **system** is reasonably interpreted as comprising a single device or multiple devices.

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

Regarding whether the DNS device is a separate device, as discussed above, the claims do not recite a particular special DNS device, much less a device physically separate from a

conventional DNS server, which is also consistent with the specification of the patent under reexamination. Indeed in one embodiment, the patent owner states "It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience." Col. 40, ll. 43-45, emphasis added.

In view of the above, it must be emphasized again that the claimed DNS "system" is interpreted reasonably broad consistent with the specification to comprise a single device (*e.g.*, a DNS server) or various combinations of multiple devices (*e.g.*, a DNS server and other DNS devices) (*e.g.*, a DNS server, a DNS proxy) (*e.g.*, a DNS server, a DNS proxy, and other DNS devices). The patent owner in their Response has not pointed to any language and arguments clearly disclaiming the embodiments discussed above that support this interpretation.

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

upon the services of a gatekeeper to receive an address (*e.g.*, a "hopblock" address, col. Col. 40, ll. 15-25) that the DNS server then provides to the initiator so that the initiator and target can establish a VPN. *See also* the Keromytis Declaration, paragraph 19.

The claims however do not recite a DNS "server" (as previously discussed) much less a DNS server that authenticates a user and relies upon the services of a gatekeeper, which is also consistent with the specification. Indeed in one embodiment, the patent owner states the DNS server (SDNS 3319) is queried "in the clear" (without using a VPN link) and without authenticating the user. Col. 51, ll. 48-61. The server then replies without the use of a gatekeeper 3314 "in the clear" so that the initiator and the target can establish a VPN. *Id.*

In view of the above, the claimed DNS system is interpreted reasonably broad consistent with the specification has not requiring a DNS server capable of authenticating the user and not requiring the services of a gatekeeper to aid in the establishment of a VPN. The patent owner in their Response has not pointed to any language and arguments clearly disclaiming the embodiments discussed above that support this interpretation.

The district court in related litigation interpreted "indication" as having no special meaning in view of the specification of the patent under reexamination and indeed the specification does not use this term specifically. Thus, the term may be construed broadly to mean a visible message or signal to a user that the DNS system supports establishing a secure

communication link. Markman Order, filed June 25, 2012 in the related *inter partes* reexamination 95/001,788 of the same patent, pp. 27 & 28.

Finally, the recited phrase "and to" means the "indication" is not explicitly tied to the "query for a network address" in any way other than that they are both part of a "system for providing a domain name service." Thus, the claims encompass a DNS system conventionally queried for a network address, where an unrelated "indication" of secure communication support is provided. That is, the claimed "indication" need not relate to the claimed "query" because the claim imposes no such requirement. The patent under reexamination not surprisingly discloses such a scenario. In "Scenario #3", the DNS system is conventionally queried for a network address based on a uniform resource locator (URL) in order to establish an unsecured connection. Col. 41, ll. 41-49. In Scenario #1," a subsequent, different request would result in an indication of secure communication (establishment of a VPN). Col. 41, ll. 23-32. The patent under reexamination also discloses an embodiment where the "indication" is only indirectly related to the original DNS query. A non-secure connection using a conventional DNS query is established either using the embodiment of "Scenario # 3" discussed above (col. 41, ll. 41-49) or that described for a non-"special user" (col. 39, ll. 46-50). Subsequently, for said unsecured connection, an "indication" of secure communication support (URL for a secure domain name service) is provided in response to a query for a secure URL (i.e., not a "query for network address) based on an unsecured domain name. Col. 50, ll. 37-45.

3.2. The Lendenmann Prior Art

3.2.A. Returning a Network Address Corresponding to a Secure Domain Name Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner asserts Lendenmann "discloses a CDS lookup process that simply returns a name, taking no measures to provide any indication that the CDS supports establishing a secure communication link." Response, p. 7. The patent owner contends this teaching fails to distinguish a conventional Domain Name Service ("DNS") system identified at col. 39, ll. 34-42 of the Larson patent under reexamination, where a DNS store public keys for different machines and allows hosts to retrieve the keys and then proceed to communicate with the different machines to establish a Virtual Private Network ("VPN"). *Id.* at 8. *See also* the Keromytis Declaration, paragraphs 27 & 28.

The third party requester is correct that the patent owner "fails to take into account the full teachings of Lendenmann with respect to the Cell Directory Service (CDS)," such as the "numerous secure communications feature that go beyond merely resolving a name into a network address." Comments, p. 3. These features will be discussed *infra*. The requester also correctly notes the patent owner's analysis lacks a comparison of the prior art to the claims at issue. *Id.* at 4.

3.2.B. The Access Control List Integrated into the Cell Directory Service Provides an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner asserts the Access Control List ("ACL") "has no bearing on the operations of the alleged domain name service system...." Response, p. 8. The "Security Service function [is]...separate from the CDS, to handle any security-related measures for communications after the CDS has returned service identification information to the client." *Id.* at 9. "Even if a client has authorization to receive the information in the CDS [Cell Directory Service], the CDS still merely 'returns the network address of the names resource'" when given a name in a request...." *Id. See also* the Keromytis Declaration, paragraph 30.

The requester however notes that Lendenmann explicitly teaches "CDS ACL management software, incorporated into all CDS clerks and servers, performs access checking for incoming requests." Lendenmann, p. 34. Comments, p. 4. Thus, the examiner agrees that the cell directory service (CDS) determines whether a user is authorized for access. Moreover, the requester correctly notes the Larson patent under reexamination "expressly states that the lack of authorization checks was a deficiency in such systems." Comments, p. 5. Indeed, the patent owner characterized DNS authorization as a distinguishing inventive feature. Keromytis Declaration, paragraph 18. See also the Response, p. 2. The Lendenmann prior art teaches a similar DNS authorization.

The patent owner also contends "[e]ven if a client has authorization to receive the information in the CDS, the CDS still merely returns the network address of the named

resource." Response, p. 9. However certain embodiments disclosed in the specification of the Larson patent under reexamination do just that. For example, the patent owner's DNS proxy 2610 answers a query by "preferably using a secure administrative VPN." Larson, col. 40, ll. 19-24. Thus, Larson discloses embodiments both using a VPN and not using a VPN, although using a VPN is preferred. Thus, Larson discloses a VPN is not required to provide the answer. *See also* col. 51, ll. 48-61, where the secure DNS server 3313 receives and answers a query "in the clear" (*i.e.*, without using a VPN) by providing the requested address. The established VPN thus completely bypasses the patent owner's DNS server.

3.2.C. Lendenmann Teaches Complete Binding Handles that Provide an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner argues Lendenmann teaches incomplete binding handles (*i.e.*, without security associations) (Response, pp. 10 & 11), but this is explicitly contradicted by Lendenmann. "Only well-known endpoints are stored in CDS. In this case, clients obtain fully bound handles." Lendenmann, p. 186. *See also* the Comments, p. 5.

3.2.D. Lendenmann Teaches an Authentication Challenge that Provides an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner argues the Remote Procedure Call ("RPC") authentication challenge is not related to CDS, thus the CDS does not provide the authentication challenge (indication) after the query. Response, pp. 11 and 12. *See also* the Keromytis Declaration, paragraph 33. Fig. 3

(p. 173) of Lendenmann however illustrates that the "Directory Service" (i.e., CDS) is based upon the RPC foundation. "This chapter discusses all components involved in the execution of an RPC, including CDS and Security Services access." *Id.* See also the Comments, p. 6.

3.2.E. Lendenmann Teaches a Server Status "Security Failures" Feature, but it is Unclear How This Feature Relates to an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

Lendenmann Teaches the Display of Online Document, but it is Unclear How This Feature Relates to an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The examiner agrees with the patent owner that Lendenmann does not adequately explained (as applied by the requester) how the server status "security failures" indication relate to an indication that the DNS system supports establishing a secure communication link. Response, pp. 12. *See also* the Keromytis Declaration, paragraphs 35 & 36. The requester discusses the ACL management software (Comments, p. 7), but this does not appear to be related to the incorporated rejection based on the "security failures" indication. *See, e.g.*, the incorporated claim chart, Exhibit F1 to the Request, p. 17. Similarly, Lendenmann fails to specifically teach that the online document provides any indication that the DNS system supports establishing a secure communication link. Response, p. 14. The online documentation of the security features providing the "indication" would also not be inherent. Lendenmann does however teach the claimed "indication" in other respects as discussed above in this section. Thus, the Lendenmann rejection is not withdrawn.

3.2.F. Dependent Claims 5, 23 and 27 are Not Patentable - Rejections Based on Lendenmann

The patent owner again argues the security service is separate from the CDS (Response, pp. 15-17), but as discussed above in section 3.2.B and as noted by the requester (Comments, p. 9), Lendenmann explicitly teaches otherwise. The requester also correctly notes the patent owner's argument is directed to unclaimed features. *Id.*

3.2.G. Dependent Claims 16, 17, 27, 33, 40, 41, 51 & 57 are Not Patentable - Rejections Based on Lendenmann

The patent owner's arguments (Response, pp. 17 & 18) appear premised on the notion that the CDS only returns incomplete bindings, which is incorrect for the reasons previously explained in section 3.2.C above. See also the Comments, p. 10.

3.2.H. Dependent Claims 24 & 48 are Not Patentable - Rejections Based on Lendenmann

The patent owner unpersuasively argues that Lendenmann fails to teach "wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." Response, pp. 18 & 19. First, Lendenmann does indeed teach that a domain names comprises an indication that the DNS system supports a secure communication link. *See, e.g.*, p. 23, "/.:/subsys/dce/sec" and "/.:/subsys/dce/sec/master." *See also* the Comments, pp. 10 & 11.

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

3.2.I. The Rejection of Claims 1-3, 5, 6, 14-30, 14-30, 33-54 and 57-60 As Obvious Over Lendenmann Is Withdrawn

The patent owner is correct that the incorporated 103 rejection over Lendenmann is deficient for failing to articulate a reason why the claimed invention would have been obvious. Response, pp. 19 & 20. For example, the 103 rejections appear to be the same as the 102 rejections except the word "teaches" has been replaced with the words "renders obvious." *Id.* It certainly cannot be the case that Lendenmann fails to "teach" any claim limitation. Thus, it is unclear as to what specific claim limitation Lendenmann fails to teach. Thus, the 103 rejection fails to ascertain the difference between the prior art and the claims, as required for a *prima facie* case of obviousness. The requester responds "[t]o the extent that Lendenmann does not anticipate the claims, Lendenmann provides an express teaching and suggestion to combine the

functionalities of its name and security servers." Comments, p. 12. This however only addresses how the prior art can be modified, but does not provide notice to the patent owner as to what specific limitation Lendenmann fails to teach and how Lendenmann would have been obviously modified to teach this specific limitation.

3.2.J. Dependent Claims 2, 3, 6, 14, 15, 18-22, 25, 26, 28-30, 34, 35, 37-39, 42-26, 52-54, 58 & 59 are Not Patentable - Rejections Based on Lendenmann

Claim 7 Is Not Patentable - Rejections Based on Obviousness Combination of Lendenmann in view of Wesinger

Claims 8 & 9 Are Not Patentable - Rejections Based on Obviousness Combination of Lendenmann in view of Gaspoz

Claim 10 Is Not Patentable - Rejections Based on Obviousness Combination of Lendenmann in view of Gaspoz and Schneider

Claims 31, 32, 5 & 56Are Not Patentable - Rejections Based on Obviousness Combination of Lendenmann in view of Ludwig and RFC 793

The patent owner's arguments (Response, pp. 19-27) appear premised on the notion that Lendenmann teaches a "separate Security Service" distinct from the CDS (e.g., Response, pp. 20-22), which the examiner does not find persuasive for the reasons previously explained in section 3.3.B above. The patent owner criticizes Gaspoz as teaching manual file creation rather than object programming is required to create a VPN in a DCE server (p. 23), but nonetheless Gaspoz teaches creating a VPN in a DCE and it is thus a suitable, secondary teaching reference.

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

The patent owner is correct that the incorporated 103 rejection over Lendenmann in view of Martin is deficient for failing to teach an "network address hopping regime that is used to pseudo randomly change network addresses in packets transmitted...." Response, pp. 24 & 25. While the requester asserts the Martin secondary reference teaches changing the source address in the packets transmitted (Comments, p. 15), the incorporated rejection does not address how this change implements a network address "hopping" regime. The term "network address *hopping* regime" cannot be meaningfully interpreted without referring to the specification, which discloses a communicating pair of nodes *hopping* to mutually agreed-upon source and destination addresses selected from a block of IP addresses using an algorithm and a randomization seed. *See* Larson, col. 39, ll. 52-55, which refers back to previous discussions of address hopping. One such discussion extensively occurs at col. 17, ll. 11-26.

3.2.L. Claims 12 & 13 Are Not Patentable - Rejections Based on Obviousness Combination of Lendenmann in view of Gaspoz and RFC 793

The patent owner argues regarding claim 12 that the TCP protocol (as evidenced by RFC 793) fails to teach a virtual private network, but the incorporated rejection relied upon the TCP protocol to teach comparing values in each data packet to a moving window of valid values. *See, e.g.*, the incorporated rejection, attached as Exhibit F-1 to the Request, pp. 138-145. The virtual private network, which runs over the TCP layer, is taught by the combination of Lendenmann in view of Gaspoz as it relates to parent claim 8. Similarly, the patent argues regarding claim 13 that RFC 793 fails to teach the "indication that the domain name service system supports

establishing a secure communication link" or that "the domain name service system is connectable to a virtual private network," but RFC 793 was not relied upon to teach these limitations. The patent owner appears to be unpersuasively attacking the references individually as asserted by the requester. Comments, pp. 16 & 17.

3.3. The Aziz Prior Art

3.3.A. The DNS System Comprises More Than Merely Name Server 120

The patent owner incorrectly characterizes the incorporated rejection as limitation the claimed "domain name service system" to Name Server (NS) 120. Response, p. 29. This is incorrect however. Although the incorporated rejection cited NS 120 as an example of a DNS system, the rejection did not limit the DNS system to a single server, which is an interpretation consistent with the specification of the Larson patent under reexamination. See section 3.1 above.

3.3.B. Returning a Network Address Corresponding to a Secure Domain Name Firewall Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner asserts the SX record, which includes the name or address of firewall 110, fails to provide an indication that the DNS system itself supports establishing a secure communication link because the firewall 110 is separate from the DNS system. Rather, Aziz teaches a conventional DNS system. Response, p. 30. *See also* the Keromytis Declaration, paragraphs 42 & 43.

The premise of the patent owner's argument is incorrect. The DNS system comprises authorized client 210 and the authorized client 210 directly establishes a secure communication with the target. The DNS system thus supports establishing a secure communication link. Specifically, the DNS system is not limited to NS 120, as discussed in section 3.3.A above. Indeed, the query initiator (authorized client 210) comprises a resolver program (name server software). Col. 6, l. 61 – col. 7, l. 7 and col. 8, ll. 28-32. The resolver is also part of the DNS system because the resolver performs the following functions: "(1) return the answer to the query if it is available locally; otherwise, (2) find the best servers to ask for the answer, (3) send queries to the servers until one responds; and (4) process the response." *Id.* Thus, the query initiator (e.g., authorized client 210) is part of the DNS system. The query initiator however also establishes the secure communication link with the target (e.g., inside host 130 and firewall 110).

Assuming incorrectly for the sake of argument client 210 is not part of the DNS system, Aziz still teaches that the DNS system supports the establishment of a secure communication link. Aziz also teaches providing an "indication" that the DNS system supports a secure communication link, such as by releasing the SX, KEY and SIG records.

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

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

Thus in Aziz, the DNS system (comprising NS 120) provides an "indication" in the form of an address of firewall 110 to which a secure communication link is established. The other information providing the "indication" (public keys, digital signature) is discussed in the next section. The DNS system itself provides an indication of support for secure communication by providing information (firewall address, keys, and digital signature) necessary for the query initiator to establish the secure communication with the target. This interpretation is also consistent with the specification of the Larson patent under reexamination, which teaches a DNS system that provides an address to the query initiator so that the initiator can establish a secure communication link to the target bypassing NS 120. For example, the Larson patent under reexamination discloses an embodiment at col. 51, ll. 11-61

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

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

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

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

3.3.C. Returning Public Keys and Digital Signatures Corresponding to a Secure Domain Name Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner asserts the KEY and SIG resource records, which includes the public key and digital signature needed to establish a secure communication, fail to provide an indication that the DNS system supports establishing a secure communication link because the firewall 110 is separate from the DNS system. Rather Aziz teaches a conventional DNS system. Response, pp. 31 & 32. *See also* the Keromytis Declaration, paragraph 45.

As discussed in section 3.3.B above, the premise of the patent owner's argument is incorrect. The DNS system comprises authorized client 210 and the authorized client 210 directly establishes a secure communication with the target. The DNS system thus supports establishing a secure communication link.

Assuming incorrectly for the sake of argument client 210 is not part of the DNS system, Aziz still teaches that the DNS system supports the establishment of a secure communication link. Aziz also teaches providing an "indication" that the DNS system supports a secure communication link, such as by releasing the SX, KEY and SIG records.

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

> To **support the need for secure communications**, a version of the Internet Domain Name System ("secure DNS") uses security extensions including KEY and SIG resource record types. The KEY resource record can be used to **distribute public keys** and associated information. That is to say, a KEY record could contain a key, a key name, or an algorithm. The SIG, or "signature," resource record can be used to **authenticate the data in other resource records**. One of the data fields in a SIG record is the "labels" field. This field is the count of how many labels are in the original SIG record owner name as it appears in the zone database (e.g., *.sun.com. has two labels because the null label (".") for root and the wildcard ("*") are not included in the count). This label count can, therefore, be used to derive the original name of a record that was retrieved as the result of wildcard substitution (to be described in detail later). The original name is needed, for example, to verify a digital signature.

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

The biggest structural difference between the Larson and Aziz teachings discussed above and in Section 3.3.B is that, in Larson, SDNS 3313 "authenticates" the query however this

feature is not recited in the independent claims. *See, e.g.*, dependent claim 5, which for the first time recites "authenticate the query..." thus implying by claim differentiation that parent, independent claim 1 need not be interpreted as requiring such an unclaimed feature. Nonetheless, as discussed above, Aziz teaches the query initiator is an "authorized" client 210.

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

3.3.D. Building Tunnel Information Tables Necessary for a Secure Connection to a Secure Domain Name Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner asserts that building information used for secure communications in the resolver program, such as tunnel information tables, fails to provide an indication that the DNS system supports establishing a secure communication link because the client 210 is separate from the DNS system. Rather Aziz teaches a conventional DNS system. Response, pp. 32 & 33.

As discussed in sections 3.3.B and 3.3.C above, the premise of the patent owner's argument is incorrect. The DNS system comprises authorized client 210 because client 210 executes a DNS resolver program. The authorized client 210 (part of the DNS system) then directly establishes a secure communication with the target. The DNS system, comprising the client, thus supports establishing a secure communication link and the prerequisite information,

such as tunnel information table residing in the client, provides an indication that the secure communication will be established.

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

Aziz teaches the security extension to DNS ("DNS-sec") (RFC 2065) in one embodiment is used to distribute the KEY and SIG records. Col. 6, ll. 11-21. Thus, the patent owner's arguments (Response, pp. 33 & 34) are unpersuasive for the reasons discussed in Section 3.3.C above, which addressed the distribution of KEY and SIG records. The examiner also agrees with the requester that the "assertion that the host speaks IPSEC" bit in the KEY record would provide an indication of support for the establishment of secure communication with the host. Comments, pp. 21 & 22. The patent owner counters the distribution of the KEY record to the query initiator does not provide an indication, so neither can the bit in question. Response, p. 33. Not only is this not true as a matter of logic (the IPSEC bit specifically can independently provide the indication), but the KEY record as a whole provides the recited indication as discussed in Section 3.3.C above.

3.3.F. The Rejection of Dependent Claims 5, 23 and 27 as Anticipated by Aziz Is Withdrawn.

The patent owner is correct that the incorporated 102 rejection over Aziz is deficient for failing to establish that the query is authenticated. While the requester notes various messages are authenticated (Comments, p. 22), Aziz fails to specifically teach that the query is

authenticated. The requester notes that RFC 2065 teaches that requests can also be authenticated "by including a special SIG RR at the end of the request" (Comments, p. 22), but Aziz fails to specifically incorporate this feature of RF 2065. Indeed, Aziz teaches "not all embodiments require such features [of secure DNS]...." Col. 6, ll. 15-21.

3.3.G. Dependent Claim 8 Is Not Patentable - Rejections Based on Aziz

Dependent Claims 17 and 41 Are Not Patentable - Rejections Based on Aziz

The patent owner's arguments (Response, pp. 35 & 36) appear premised on the idea that the DNS system is limited to NS 120 and furthermore that the DNS system does not support the establishment of a secure network or indications thereof, which is incorrect for the reasons previously explained in section 3.3.A-E above. See also the Comments, pp. 22 & 23.

3.3.H. Dependent Claims 18 and 42 Are Not Patentable - Rejections Based on Aziz

The patent owner contends Aziz fails to teach a domain name reserved for secure communication link (Response, pp. 36 & 37), but Aziz teaches "network administrator may sometimes also want to permit authorized clients outside the protected zone to communicate with hosts inside the protected zone" (col. 2, ll. 20-22), which Aziz achieves by use of a firewall 110 to handle encrypted communication between an "authorized" client 210 and a host inside protected zone 180 (Fig. 1 and col. 9, ll. 5-7). A host inside the "protected zone" however corresponds to domain names, such as eng.sun.com and corp.sun.com. Col. 1, ll. 58-60. Thus, domain names, such as eng.sun.com, are reserved to a protected zone for the possibility of secure

communications with an outside, authorized client, although certainly the initiator is not required to then establish a secure communication link (i.e., take advantage of the reserved domain name). See also the Comments, pp. 23 & 24.

3.3.I. Dependent Claims 24 and 48 Are Not Patentable - Rejections Based on Aziz

The patent owner unpersuasively argues that Aziz fails to teach "wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." Response, pp. 37 & 38. *See also* the Keromytis Declaration, paragraph 91. A "name" indicating that the DNS supports a secure communication link is nonfunctional descriptive material and thus cannot distinguish over the prior art. A "name" comprising an "indication" (as broadly recited) of support for a secure communications link is descriptive material directed to the mere arrangement of data. It is not a data structure (physical or logical relationships among data elements designed to support specific data manipulation functions) that defines a functional interrelationship to a secure communications function. MPEP 2106.01. In order to claim functional descriptive material, the claim should explicitly recite a data structure, such as a domain name comprising a secure top-level domain name (*e.g.*, ".scom" Larson, col. 50, ll. 25-37) and explicitly recite a functional relationship that interrelates the secure top-level domain name to the establishment of a secure communications link.

3.3.J. The Rejection of Dependent Claim 50 as Anticipated by Aziz Is Withdrawn.

The requester admits the proposed rejection of claim 50 as anticipated by Aziz was made in error. Comments, p. 25. Thus, this rejection is withdrawn.

3.3.K. Dependent Claims 2, 6, 7, 14, 15, 19-22, 24, 25, 27, 33-40, 43-46, 49, 51, 52, 58 and 59 Are Not Patentable - Rejections Based on Aziz

The patent owner's arguments (Response, p. 39) are based upon the limitations of the parent claims, which were found unpersuasive for the reasons previously explained in section 3.3.A-E above.

3.3.L. The Rejection of Claims 1, 2, 5-9, 14-25, 27, 28, 33-52 and 57-60 As Obvious Over Aziz Is Withdrawn

The patent owner is correct that the incorporated 103 rejection over Aziz is deficient for failing to articulate a reason why the claimed invention would have been obvious. Response, pp. 39 & 40. For example, the 103 rejections appear to be the same as the 102 rejections except the word "teaches" has been replaced with the words "renders obvious." *Id.* It certainly cannot be the case that Aziz fails to "teach" any claim limitation. Thus, it is unclear as to what specific claim limitation Aziz fails to teach. Thus, the 103 rejection fails to ascertain the difference between the prior art and the claims, as required for a *prima facie* case of obviousness. The requester responds "[t]o the extent that Aziz does not anticipate the claims, Aziz suggests that a domain name server can have security records defined to allow it to participate in a secure communication link, and further that the domain name server may handle the secure

communications itself." Comments, pp. 26 & 27. This however only addresses how the prior art can be modified, but does not provide notice to the patent owner as to what specific limitation Aziz fails to teach and how Aziz would have been obviously modified to teach this specific limitation.

3.3.M. Dependent Claims 3, 4 and 26 Are Not Patentable - Rejections Based on Aziz in view of Lawton

The patent owner incorrectly asserts that Aziz fails to teach a domain name that enables establishment of a secure communication link. Response, pp. 40-42. As explained in section 3.3.B above, Aziz teaches that the SX record is returned with the address corresponding to a domain name query. See also col. 6, ll. 48-50. RFC 2065 (DNS-sec) in one embodiment is used to implement the KEY and SIG resource records. Col. 6, ll. 11-23. In DNS-sec, the public key "must be included if space is available" in a type "A" (host address) response record (section 3.7). See RFC 2065, of record in this proceeding. As also explained in sections 3.3.B and C, the SX and KEY records provide for the establishment of a secure communication link. Thus, in Aziz a domain name enables establishment of a secure communication link. The requester relied upon Lawton to teach publication of a protected domain name so that the domain name would obviously be used enable a secure communication from outside the protected network. Comments, pp. 27 & 28.

3.3.N. Dependent Claim 9 Is Not Patentable - Rejections Based on Aziz in view of Franaszek

The patent owner argues the combination of Aziz in view of Franaszek would have changed the principle of operation of Aziz and moreover Franaszek is nonanalogous art. Response, pp. 42-46. Although the examiner agrees that Franaszek is somewhat further afield than a secondary reference directed to network communications would be, Franaszek is merely being relied upon to teach organizing a plurality of communication paths (which are taught by Aziz) into a hierarchy. Such a broad concept - the need to organize communication paths into a hierarchy – is applicable to both communication networks and computer networks. Moreover, this broad concept, when added to Aziz, does not require Aziz to change its principle of operation. The communication networks taught by Aziz alone would simply be organized hierarchically after the modification. The patent owner also asserts Franaszek is nonanalogous art because it is not reasonably pertinent to the problem recited in the claim of the patent under reexamination, however this is unpersuasive this problem - a need for "easy and convenient" communications - is not claimed, and thus the patent owner's arguments are essentially directed to unclaimed features. Comments, p. 30.

3.3.O. Dependent Claim 10 Is Not Patentable - Rejection Based on Aziz in View of Schneier

The patent owner's arguments (Response, p. 46) are based upon the limitations of the parent claims, which were found unpersuasive for the reasons previously explained in section 3.3.A-E above.

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

The patent owner is correct that the incorporated 103 rejection over Aziz in view of Martin is deficient for failing to teach an "network address hopping regime that is used to pseudo randomly change network addresses in packets transmitted...." (claim 11) and "comparing a value in each data packet transmitted...." (claim 12). Response, pp. 46-48. While the requester asserts the Martin secondary reference teaches changing the source address in the packets transmitted (Comments, pp. 31 & 32), the incorporated rejection does not address how this change implements a network address "hopping" regime. The term "network address *hopping* regime" cannot be meaningfully interpreted without referring to the specification, which discloses a communicating pair of nodes *hopping* to mutually agreed-upon source and destination addresses selected from a block of IP addresses using an algorithm and a randomization seed. *See* Larson, col. 39, ll. 52-55, which refers back to previous discussions of address hopping. One such discussion extensively occurs at col. 17, ll. 11-26. Regarding claims 12 and 13, the incorporated rejection admits that neither Aziz or Martin teach comparing the source of the data packets ("value in each data packet") as coming from one of the range of valid values recited in the claims ("moving window of valid values") or comparing a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for a first device. See, e.g., pages 99 and 100 of the incorporated claim chart attached as Exhibit F-2 to the Request.

3.3.Q. Dependent Claims 29-32 and 53-56 Are Not Patentable - Rejections Based on Aziz in View of Ludwig

The patent owner's arguments (Response, pp. 48 & 49) are based upon the limitations of the parent claims, which were found unpersuasive for the reasons previously explained in section 3.3.A-E above.

3.4. The Kiuchi and Pfaffenberger Prior Art

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

The patent owner asserts returning the public key of the secure server-side proxy fails to provide an indication that the DNS system itself supports establishing a secure communication link because the secured server-side proxy is separate from the DNS system. Rather, Kiuchi teaches a conventional DNS system. Response, pp. 51 & 52. *See also* the Keromytis Declaration, paragraph 56 & 57.

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

Considering only the public key or the moment (the IP address will be addressed in the subsequent section), Kiuchi explicitly teaches that releasing the public key of the secure server-

side proxy provides an indication that the DNS system supports a secure communication link (p. 65, section 2) (emphasis added):

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

Thus in Kiuchi, the DNS system (comprising the C-HTTP name server) provides an "indication" in the form of public key of a secure server-side proxy to which a secure communication link is established. The other information providing the "indication" (IP address and nonce values) is discussed in the next section. The DNS system itself provides an indication of support for secure communication by providing information (public keys, IP address, nonce values) necessary for the query initiator to establish the secure communication with the target. This interpretation is also consistent with the specification of the Larson patent under reexamination, which teaches a DNS system that provides an address to the query initiator so that the initiator can establish a secure communication link to the target bypassing NS 120. For example, the Larson patent under reexamination discloses an embodiment at col. 51, ll. 11-61:

> SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure

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

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

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

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

See also the Comments, pp. 34-36. The requester's correctly notes that the DNS system (comprising the C-HTTP name server) itself participates in a secure communications link,

although such a direct participation is not required according to a reasonably broad interpretation of the claims consistent with the specification, as discussed above.

3.4.B. Returning a IP Address of a Secured Proxy Server Teaches an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The patent owner offers similar reasons to those addressed in section 3.4.A as to why the IP address fails to provide the claimed indication. Response, pp. 52 & 53. *See also* the Keromytis Declaration, paragraph 58. The examiner finds the present arguments unpersuasive for similar reasons. The examiner notes that the release of the IP address by the C-HTTP name server cannot be viewed in isolation as a conventional domain name query for an IP address. As discussed above, Kiuchi teaches that if a connection to the secure server-side proxy corresponding to the IP address, then the C-HTTP releases an error code and subsequently performs a conventional DNS lookup. Thus, the release of the IP address is in the context of an unconventional DNS lookup for the purpose of determining whether the DNS system can support establishing a secure communication link by releasing the necessary public key, IP address, and nonce value.

3.4.C. There Are No Deficiencies in Kiuchi For Pfaffenberger to Remedy

The patent owner contends Pfaffenberger fails to remedy the deficiencies in Kiuchi (Response, pp. 53-55), but as discussed in sections 3.4.A and B above, Kiuchi is not deficient in the manner asserted by the patent owner.

3.4.D. The Combination of Kiuchi and Pfaffenberger Would Have Been Obvious

The patent owner argues the combination of Kiuchi in view of Pffafenberger would not have been obvious because Pfaffenberger is nonanalogous art because it is not reasonably pertinent to the problem recited in the claim of the patent under reexamination. Response, pp. 55 & 56. This argument is unpersuasive however because the asserted problem - a need for "easy and convenient" communications - is not claimed, and thus the patent owner's arguments are essentially directed to unclaimed features. See also the Comments, p. 38.

3.4.E. Dependent Claims 8, 9, 10, 12 and 13 - Rejections Based on Kiuchi in View of Pfaffenberger

Regarding claims 8, 9, 10, and 12, the patent owner advances a series of arguments as to why Kiuchi fails to teach a specific implementation of the claimed virtual private network. Response, pp. 56-58. *See also* the Keromytis Declaration, paragraph 77. As noted by the requester however, "the claims simply recite a 'virtual private network,' and introducing a new limitation regarding a specific implementation of a virtual private network (that is not described in the specification), such as a 'virtual private network implemented not via point-network links' would be erroneous." Comments, p. 40. Kiuchi teaches "[u]sing C-HTTP, a closed HTTP-based virtual network can be constructed for closed groups....." P. 60, emphasis added. Kiuchi is also clearly directed toward using C-HTTP to provide a private network for sensitive data, such as medical data. Thus, Kiuchi explicitly teaches that C-HTTP is used to establish a virtual private network.

Regardless however, the patent owner's specific implementation of a virtual private network, which the patent owner wishes to improperly read into the claims, is simply not representative of a virtual private network, which at its most basic level is point-to-point. See, e.g., Exhibits G & H provided by the requester. Comments, p. 40 including FN 5. In addition, Exhibit H teaches that the IPSec protocol is used to implement a VPN. One of ordinary skill would understand that IPSec relies upon the establishment of point-to-point and even simplex (*i.e.*, unidirectional) security associations ("SA") between edge-devices capable of implementing VPN services (e.g., IPSec capable edge routers). It is the security association database (software) that allows the merging of multiple, point-to-point SA(s). *See, e.g.*, RFC 2401 "Security Architecture for the Internet Protocol" (November 1998), of record in the related *inter partes* 95/001,788 reexamination of the same patent.

Regarding again claims 10, 12 and 13, the patent owner argues that Kiuchi as modified fails to teach "inserting into each data packet communicated...data values that vary according to a pseudo-random sequence" (claim 10), "comparing a value in each data packet transmitted...to a moving window of valid values" (claim 12), and "comparison of a discriminator field in a header of each data packet to a table of valid discriminator fields..." (claim 13). The patent owner argues, for example, that the requester asserts Kiuchi teaches the "inserting" and "comparing" in regard to signaling requests and responses, but not into "each" data packet (*i.e.*, both the signaling and non-signaling data packets) as claimed. Response, pp. 59-63. The examiner agrees. The requester counters the signaling messages (e.g., queries/responses) in

Kiuchi are part of the VPN (Comments, p. 42), but that still does not teach that the "inserting" and "comparing" happens to each packet in the VPN as claimed. The requester also argues it would have been obvious to perform the recited inserting and comparing for each data packet (*id.*), but does not identify what prior art (e.g., secondary reference) teaches doing so for every packet in the VPN. Regarding claim 12, the examiner agrees with the patent owner that Kiuchi fails to clearly teach "how the values of the Nonce header field are checked, and certainly does not teach that they are checked by comparing them to "a moving window of valid values." Response, p. 61. Thus, the rejections of claims 10, 12 and 13 as being over Kiuchi in view of Pffafenberger are withdrawn.

3.4.F. Dependent Claims 17 and 41 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger

The patent owner's arguments (Response, p. 63) are based upon the limitations of the parent claims, which were found unpersuasive for the reasons previously explained in section 3.3.A and B above.

3.4.G. Dependent Claims 24 and 48 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger

The patent owner unpersuasively argues that Kiuchi fails to teach "wherein at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link." Response, pp. 63. However, Kiuchi teaches the domain name for a secured C-HTTP host is "another.server.in.closed.network" but this domain name is for a server in the secure network and therefore "indicates nothing regarding

the capabilities of the alleged domain name service system." *Id.* at 64. The examiner does not agree. Clearly, the domain name "another.server.in.closed.network" provides an indication that the host (server) corresponding to name (closed) is secure at least to the extent it is "closed." The name server (within the DNS system) resolves the name into an address and public key corresponding to the secure host in order to support the establishment of a connection to the secure (closed) server. The domain name therefore also indicates that a DNS system will resolve the domain name into an IP address and public key to support the establishment of a connection to the secure (closed) server. See also the Comments, pp. 44 & 45.

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

3.4.J. Dependent Claims 26 and 27 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger

The patent owner incorrectly asserts that Kiuchi fails to teach a domain name that enables establishment of a secure communication link. Response, pp. 64-65. As explained in section 3.4.A & B above, Kiuchi teaches that a public key and nonce value is returned with the address corresponding to a domain name query. As also explained, the public key, IP address (instead of an error message) and the nonce value provide for the establishment of a secure communication link. Thus, in Kiuchi a domain name enables establishment of a secure communication link.

3.4.K. Dependent Claims 2-4, 7, 11, 14-16, 18, 19, 22, 25, 28-30, 33, 34, 37-40, 42, 43, 46, 49-54 and 57-69 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger

Dependent Claims 5, 23, and 47 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger and Rivest

Dependent Claim 7 Is Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger and Borella

The patent owner's arguments (Response, pp. 65-67) are based upon the limitations of the parent claims, which were found unpersuasive for the reasons previously explained in section 3.3.A and B above.

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

The patent owner is correct that the incorporated 103 rejection over Kiuchi in view of Pfaffenberger and Martin is deficient for failing to teach an "network address hopping regime that is used to pseudo randomly change network addresses in packets transmitted...." (claim 11).

While the requester asserts the Martin secondary reference teaches changing the source address in the packets transmitted (Comments, p. 47), the incorporated rejection does not address how this change implements a network address "hopping" regime. The term "network address *hopping* regime" cannot be meaningfully interpreted without referring to the specification, which discloses a communicating pair of nodes *hopping* to mutually agreed-upon source and destination addresses selected from a block of IP addresses using an algorithm and a randomization seed. *See* Larson, col. 39, ll. 52-55, which refers back to previous discussions of address hopping. One such discussion extensively occurs at col. 17, ll. 11-26.

3.4.M. Dependent Claims 20, 21, 35, 44 and 45 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger and Broadhurst

Dependent Claims 31, 33, 35 and 56 Are Not Patentable - Rejections Based on Kiuchi in View of Pfaffenberger and Ludwig

The patent owner's arguments (Response, p. 68) are based upon the limitations of the parent claims, which were found unpersuasive for the reasons previously explained in section 3.3.A and B above.

3.5. Secondary Considerations of Non-obviousness

The patent owner has not established a *nexus* between the secondary evidence and the claimed invention. MPEP 716.01.b. The patent owner argues there is substantial evidence of secondary considerations to demonstrate nonobviousness regarding "any of claims 1-60," but fails to describe how the evidence specifically relates to the subject matter of any of the claims. Response, pp. 69-71. The Declaration by Robert Dunham Short III, filed with the Response, (the

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

As noted by the requester (Comment, p. 48), the alleged need for a "system that could be easily and correctly used to enable secure communications" is such a broad need that the patent owner has not demonstrated whether the prior art, such as Lendenmann, Aziz, Kiuchi and Pfaffenberger, satisfied this need. If limitations such as "an indication that the domain name service system supports establishing a secure communication link" identified by the patent owner allow the user to in some unspecified manner to "easily" and "correctly" enable secure communications, then it would seem various prior art DNS security feature in the applied prior art would also allow the user to "easily" and "correctly" enable secure communications in a same, similar or different manner. The long-felt need must not have been satisfied by another before the invention by patent owner. MPEP 716.04.II.

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

established a *nexus* between the evidence of commercial success and the claims of the patent under reexamination.

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

4. Information Disclosure Statement

The Information Disclosure Statement ("IDS") filed April 25, 2012 citing approximately 1,325 references, has been considered. The examiner however notes that MPEP 2656, under the heading "Prior Art Patents and Printed Publications Reviewed by Examiner in Reexamination" states, in part (emphasis added):

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

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

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

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

5. Conclusion

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

(1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.

(2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).

(3) Appeal **cannot** be taken from this action, since it is not a final Office action.

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

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

Extensions of time under 37 CFR 1.136(a) will not be permitted in *inter partes* reexamination proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to the patent owner in a reexamination proceeding. Additionally, 35 U.S.C. 314(c) requires that *inter partes* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.937). Patent owner extensions of time in *inter partes* reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner's response is set by statute. 35 U.S.C. 314(b)(3).

The patent owner is reminded of the continuing responsibility under 37 CFR 1.985(a), to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent undergoing reexamination or any related patent throughout the course of this

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

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

By Mail to:	Mail Stop *Inter Partes* Reexam Attn: Central Reexamination Unit Commissioner of Patents United States Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450
By FAX to:	(571) 273-9900 Central Reexamination Unit
By hand:	Customer Service Window Randolph Building 401 Dulany St. Alexandria, VA 22314

By EFS-Web:

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

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

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

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

Signed:
/Roland G. Foster/
Roland G. Foster
Central Reexamination Unit, Primary Examiner
Electrical Art Unit 3992
(571) 272-7538

Conferee: /BJP/

Conferee: /DJR/

Re Exam

Sheet 1 of 39

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Pat Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	60/151,563	08/31/1999	Bryan Whittles	
	A3	60/134,547	05/17/1999	Victory Sheymov	
	A4	2,895,502	07/21/1959	Roper et al.	
	A5	4,761,334	08/1988	Sagoi et al.	
	A6	4,885,778	12/5/1989	Weiss, Kenneth	
	A7	4,920,484	4/24/1990	Ranade	
	A8	4,933,846	06/12/1990	Humphrey et al.	
	A9	4,952,930	08/28/1990	Franaszek et al.	
	A10	4,988,990	01/29/1991	Warrior	
	A11	5,164,988	11/17/1992	Matyas	
	A12	5,204,961	04/20/1993	Barlow	
	A13	5,276,735	01/04/1994	Boebert et al	
	A14	5,303,302	04/12/1994	Burrows	
	A15	5,311,593	05/10/1994	Carmi	
	A16	5,329,521	07/12/1994	Walsh et al.	
	A17	5,341,426	08/23/1994	Barney et al.	
	A18	5,367,643	11/22/1994	Chang et al	
	A19	5,384,848	01/24/1995	Kikuchi	
	A20	5,511,122	04/23/1996	Atkinson	
	A21	5,548,646	08/20/1996	Aziz et al.	
	A22	5,559,883	09/24/1996	Williams	
	A23	5,561,669	10/01/1996	Lenney et al	
	A24	5,588,060	12/24/1996	Aziz	
	A25	5,590,285	12/31/1996	Krause et al.	
	A26	5,625,626	04/29/1997	Umekita	
	A27	5,629,984	05/13/1997	McManis	
	A28	5,654,695	08/05/1997	Olnowich et al	
	A29	5,682,480	10/28/1997	Nakagawa	
	A30	5,689,566	11/18/1997	Nguyen	
	A31	5,689,641	11/18/1997	Ludwig et al.	
	A32	5,740,375	04/14/1998	Dunne et al.	
	A33	5,757,925	05/1998	Faybishenko	
	A34	5,764,906	06/1998	Edelstein et al.	
	A35	5,771,239	06/23/1998	Moroney et al.	
	A36	5,774,660	6/30/1998	Brendel et al	
	A37	5,787,172	07/28/1998	Arnold	
	A38	5,790,548	08/04/1998	Sitaraman et al.	
	A39	5,796,942	08/18/1998	Esbensen	
	A40	5,805,801	09/08/1998	Holloway et al.	
	A41	5,805,803	09/08/1998	Birrell et al.	
	A42	5,822,434	10/13/1998	Caronni et al.	
	A43	5,842,040	11/24/1998	Hughes et al.	
	A44	5,845,091	12/01/1998	Dunne et al.	
	A45	5,864,666	01/1999	Shrader, Theodore Jack London	
	A46	5,867,650	02/02/1998	Osterman	
	A47	5,870,610	02/09/1999	Beyda et al.	
	A48	5,878,231	05/02/1999	Baehr et al	
	A49	5,892,903	04/06/1999	Klaus	
	A50	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A51	5,905,859	05/18/1999	Holloway et al.	
	A52	5,919,018	06/29/1999	Goedgrup et al	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Complete if Known

Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A53	5,918,019	06/29/1999	Valencia	
	A54	5,950,195	09/07/1999	Stockwell et al.	
	A55	5,950,519	09/14/1999	Anatoli	
	A56	5,960,204	09/28/1999	Yinger et al.	
	A57	5,996,016	11/30/1999	Thalheimer et al.	
	A58	6,006,259	12/21/1999	Adelman et al.	
	A59	6,006,272	12/21/1999	Aravamudan et al	
	A60	6,016,318	01/18/2000	Tomoike	
	A61	6,016,512	01/18/2000	Huitema	
	A62	6,041,342	03/21/2000	Yamaguchi	
	A63	6,052,788	04/2000	Wesinger et al.	
	A64	6,055,574	04/25/2000	Smorodinsky et al.	
	A65	6,061,346	05/2000	Nordman, Mikael	
	A66	6,061,736	05/09/2000	Rochberger et al	
	A67	6,079,020	06/20/2000	Liu	
	A68	6,081,900	06/2000	Subramaniam et al.	
	A69	6,092,200	07/18/2000	Muniyappa et al.	
	A70	6,101,182	08/2000	Sistanizadeh et al.	
	A71	6,119,171	09/12/2000	Alkhatib	
	A72	6,119,234	09/12/2000	Aziz et al.	
	A73	6,131,121	10/10/2000	Mattaway et al.	
	A74	6,147,976	11/14/2000	Shand et al.	
	A75	6,157,957	12/05/2000	Berthaud	
	A76	6,158,011	12/05/2000	Chen et al.	
	A77	6,168,409	01/02/2001	Fare	
	A78	6,173,399	01/09/2001	Gilbrech	
	A79	6,175,867	01/16/2001	Taghadoss	
	A80	6,178,409	01/23/2001	Weber et al.	
	A81	6,178,505	01/23/2001	Schneider et al	
	A82	6,179,102	01/30/2001	Weber, et al.	
	A83	6,182,141	1/30/2001	Blum et al.	
	A84	6,199,112	03/2001	Wilson, Stephen K.	
	A85	6,202,081	03/2001	Naudus, Stanley T.	
	A86	6,222,842	04/24/2001	Sasyan et al.	
	A87	6,223,287	04/24/2001	Douglas et al.	
	A88	6,226,748	05/01/2001	Bots et al.	
	A89	6,226,751	05/01/2001	Arrow et al..	
	A90	6,233,618	05/15/2001	Shannon	
	A91	6,243,360	06/05/2001	Basilico	
	A92	6,243,749	06/05/2001	Sitaraman et al.	
	A93	6,243,754	06/05/2001	Guerin et al	
	A94	6,246,670	06/12/2001	Karlsson et al.	
	A95	6,256,671	07/03/2001	Strentzsch et al.	
	A96	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A97	6,263,445	07/17/2001	Blumenau	
	A98	6,269,099	07/31/2001	Borella et al.	
	A99	6,286,047	09/04/2001	Ramanathan et al	
	A100	6,298,341	10/02/01	Mann, et al.	
	A101	6,301,223	10/9/2001	Hrastar et al	
	A102	6,308,213	10/23/2001	Valencia	
	A103	6,308,274	10/23/2001	Swift	
	A104	6,311,207	10/30/2001	Mighdoll et al	
	A105	6,314,463	11/2001	Abbott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Sheet 1 of 44

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A106	6,324,161	11/27/2001	Kirch	
	A107	6,330,562	12/11/2001	Boden et al.	
	A108	6,332,158	12/18/2001	Risley et al.	
	A109	6,333,272	12/25/01	McMillin, et al.	
	A110	6,338,082	01/08/02	Schneider, Eric	
	A111	6,353,614	03/05/2002	Borella et al.	
	A112	6,425,003	07/23/2002	Herzog et al.	
	A113	6,430,155	08/06/2002	Davie et al	
	A114	6,430,610	08/06/2002	Carter	
	A115	6,487,598	11/26/2002	Valencia	
	A116	6,496,867	12/17/2002	Beser et al.	
	A117	6,499,108	12/24/2002	Johnson	
	A118	6,502,135	12/2002	Munger et al.	
	A119	6,505,232	01/07/2003	Mighdoll et al	
	A120	6,510,154	01/21/2003	Mayes et al	
	A121	6,549,516	04/15/2003	Albert et al	
	A122	6,557,037	04/2003	Provino, Joseph E.	
	A123	6,560,634	05/06/2003	Broadhurst	
	A124	6,571,296	05/27/2002	Dillon	
	A125	6,571,338	05/27/2003	Shaio et al.	
	A126	6,581,166	7/17/2003	Hirst et al.	
	A127	6,606,708	08/12/2003	Devine et al.	
	A128	6,615,357	9/2/2003	Boden et al.	
	A129	6,618,761	09/09/2003	Munger et al.	
	A130	6,671,702	12/30/2003	Kruglikov et al	
	A131	6,687,551	2/3/2004	Steindl	
	A132	6,687,746	02/03/04	Shuster, et al.	
	A133	6,701,437	03/02/2004	Hoke et al.	
	A134	6,714,970	3/30/2004	Fiveash et al.	
	A135	6,717,949	4/6/2004	Boden et al.	
	A136	6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A137	6,752,166	06/22/04	Lull, et al.	
	A138	6,757,740	06/29/04	Parekh, et al.	
	A139	6,760,766	7/6/2004	Sahlqvist	
	A140	6,813,777	11/2004	Weinberger et al.	
	A141	6,826,616	11/30/2004	Larson et al.	
	A142	6,839,759	1/4/2005	Larson et al.	
	A143	6,937,597	08/30/2005	Rosenberg et al.	
	A144	7,010,604	3/7/2006	Munger et al.	
	A145	7,039,713	05/2006	Van Gunter et al.	
	A146	7,072,964	07/04/2006	Whittle et al.	
	A147	7,133,930	11/7/2006	Munger et al.	
	A148	7,167,904	01/23/07	Devarajan, et al.	
	A149	7,188,175	03/06/07	McKeeth, James A.	
	A150	7,188,180	3/6/2007	Larson et al.	
	A151	7,197,563	3/27/2007	Sheymov et al.	
	A152	7,353,841	04/08/08	Kono, et al.	
	A153	7,418,504	08/2008	Larson et al.	
	A154	7,461,334	12/02/08	Lu, et al.	
	A155	7,490,151	02/2009	Munger et al.	
	A156	7,493,403	02/2009	Shull et al.	
	A157	7,584,500	09/2009	Dillon et al.	
	A158	7,764,231	07/27/2010	Karr et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	**Complete if Known**
	Application Number: **95/001,851**
	Filing Date: **December 13, 2011**
	First Named Inventor: **Victor Larson**
	Art Unit: **3992**
	Examiner Name: **Roland G. Foster**
	Docket Number: **11798.0007-00000**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A159	7,852,861	12/2010	Wu et al.	
	A160	7,921,211	04/2011	Larson et al.	
	A161	7,933,990	04/2011	Munger et al.	
	A162	8,051,181	11/2011	Larson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2002/0004898	1/10/02	Droge	
	B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
	B4	US2004/0199493	10/2004	Ruiz et al.	
	B5	US2004/0199520	10/2004	Ruiz et al.	
	B6	US2004/0199608	10/2004	Rechterman et al.	
	B7	US2004/0199620	10/2004	Ruiz et al.	
	B8	US2005/0055306	3/10/05	Miller et al.	
	B9	US2005/0108517	05/2005	Dillon et al.	
	B10	US2006/0059337	03/16/2006	Polyhonen et al.	
	B11	US2006/0123134	06/2006	Munger et al.	
	B12	US2007/0208869	09/2007	Adelman et al.	
	B13	US2007/0214284	09/2007	King et al.	
	B14	US2007/0266141	11/2007	Norton, Michael Anthony	
	B15	US2008/0005792	01/2008	*Larson et al.	
	B16	US2008/0144625	06/2008	Wu et al.	
	B17	US2008/0235507	09/2008	Ishikawa et al.	
	B18	US2009/0193498	07/2009	Agarwal et al.	
	B19	US2009/0193513	07/2009	Agarwal et al.	
	B20	US2009/0199258	08/2009	Deng et al.	
	B21	US2009/0199285	09/2009	Agarwal et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Receipt date: 04/25/2012 95001851 - GAU: 3992

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,746
	Filing Date	September 7, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Andrew L. Nalven
	Docket Number	11798.0007-00000

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 – Number 4 –Kind Code5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	DE19924575	12/2/99	Provino et al.			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	EP0838930	4/29/1988	Digital Equipment Corporation			
	C4	EP0858189	8/12/98	Maciel et al.			
	C5	EP836306	4/15/1998	HEWLETT PACKARD CO			
	C6	GB2317792	04/01/1998	Secure Computing Corporation			
	C7	GB2334181	08/11/1999	NEC Technologies			
	C8	GB2340702	02/23/2000	Sun Microsystems Inc.			
	C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp			
	C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp			
	C11	JP10-070531	03/10/1998	Brother Ind Ltd.			
	C12	JP62-214744	9/21/1987	Hitachi Ltd.			
	C13	WO0070458	11/23/2000	Comsec Corporation			
	C14	WO0017775	3/30/00	Miller et al.			
	C15	WO01016766	03/08/2001	Science Applications International Corporation			
	C16	WO0150688	7/12/01	Kriens			
	C17	WO9827783	06/25/1998	Northern Telecom Limited			
	C18	WO9855930	12/10/98	Tang			
	C19	WO9843396	10/01/1998	Northern Telecom Limited			
	C20	WO9859470	12/30/98	Kanter et al.			
	C21	WO9911019	03/04/1999	V One Corp			
	C22	WO9938081	7/29/99	Paulsen et al.			
	C23	WO9948303	9/23/99	Cox et al.			
	C24	WO01/61922	02/12/2001	Science Application International Corporation			

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

EXAMINER'S INITIALS	CITE NO.	OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.) Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D4	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	D6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D8	F. Halsall,."Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D9	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D10	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	D11	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	D12	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D13	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D14	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	D15	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D16	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D17	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	D18	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	D19	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	D20	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D21	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D22	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D23	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	
	D24	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D25	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	D26	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D27	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**95/001,851**
				Filing Date	**December 13, 2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**3992**
				Examiner Name	**Roland G. Foster**
				Docket Number	**11798.0007-00000**

		SIGCOMM conference on Communications architectures & protocols. pp. 84-91, ACM Press, NY, NY 1986.	
	D28	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D29	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	D30	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation.	
	D31	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D32	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D33	I. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) RFC1101, DNS SRV)	
	D34	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	D35	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	D37	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	D38	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	D39	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	D40	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	D41	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	D42	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	D43	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	
	D44	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	D45	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	D46	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	D47	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista)	
	D48	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	D49	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	D50	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)	
	D51	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/19970620030031 2/www.aventail.com/educate/whitepaper/ipmw.html (1997). (Corporate Access, Aventail)	
	D53	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	D54	Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschtag I, Onion Routing)	
	D55	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	D62	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	D63	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	D64	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	D65	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Definition, ANX)	
	D66	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	D67	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	
	D68	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	D69	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	D70	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	D71	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	D72	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	D73	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured there from and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	D74	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D75	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (*available at* http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue). (NT Beta, Microsoft Prior Art VPN Technology)	
	D76	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	D77	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	D78	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	D79	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	D80	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	D81	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). DISA, SIPRNET)	
	D82	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	D83	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	D84	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	D85	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	D86	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	D87	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	D88	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	D89	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	D90	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	D91	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	D92	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	D93	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	D94	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	D95	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	D96	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	D97	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	D98	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	D99	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*,<draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). Scott VPNs)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**95/001,851**
				Filing Date	**December 13, 2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**3992**
				Examiner Name	**Roland G. Foster**
				Docket Number	**11798.0007-00000**

	D101	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	D102	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	D103	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	D104	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	D105	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	D106	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	D107	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	D108	Bhattacharya, et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	D109	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	D110	Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D111	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	D112	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	D113	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	D114	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	D115	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	D116	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	D117	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	D118	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	D119	Assured Digital Products. (Assured Digital)	
	D120	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	D121	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	D122	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	D123	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	D124	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	D125	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	
	D126	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	D127	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	D128	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	D129	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	D130	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D131	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	D132	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	D140	Dan Sterne *et al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	D142	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	D143	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	D144	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	D145	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D147	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D148	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D149	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	D150	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	**Complete if Known**
	Application Number: **95/001,851**
	Filing Date: **December 13, 2011**
	First Named Inventor: **Victor Larson**
	Art Unit: **3992**
	Examiner Name: **Roland G. Foster**
	Docket Number: **11798.0007-00000**

	D154	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	D162	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/techneUarchive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	D165	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	D168	Kenneth Gregg, *et al., Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/enus/library/bb545687(VS.85.printer).aspx (Remote Access)	
	D170	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D171	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D172	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch0l.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D175	F-Secure, *F-Secure NameSurfer*(May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) F-Secure VPN 3)	
	D177	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	D185	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	D187	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	D189	F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., *SafeNet/Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	D198	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Sheet for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D204	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	D205	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	D206	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	D207	Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0* (September 21, 1998)	
	D209	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	D210	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	D211	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	D212	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	D213	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	D214	*Virtual Private Network Demonstration* (March 21, 1998)	
	D215	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	D216	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	D217	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	D218	Information Assurance, *Science Fair Agenda* (2000)	
	D219	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	D220	*IFE 3.1 Technology Dependencies* (2000)	
	D221	*IFE 3.1 Topology* (February 9, 2000)	
	D222	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	D224	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	D225	Information Assurance/NAI Labs, Dynamic Virtual Private Networks Presentation v.3 (2000)	
	D226	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	D228	Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, *MCSE Test Success: Proxy Server 2*(1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D238	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000	

~~ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH~~. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D239	*AutoSOCKS v2. 1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers, 1 99x/msg00945.html	
	D241	FirstVPN Enterprise Networks, Overview	
	D242	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	D243	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	D244	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	D245	Virtual Private Networks - Assured Digital Incorporated - ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	D246	Accessware - The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	D247	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	D248	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	D250	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
	D256	Davies and Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
	D257	Davies et al., "An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer," Security for Computer Networks, Second Edition, pp. 98-101 (1989)	
	D258	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)	
	D259	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)	
	D260	Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D261	De Raadt et al., "Cryptography in OpenBSD," 9 pages (1999)	
	D262	Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	
	D263	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	D264	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D265	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D266	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	D267	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D268	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	D269	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D270	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D271	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D272	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D273	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages.	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages.	
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages.	
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	
	D299	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	
	D300	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D301	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D302	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D303	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D304	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D305	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D306	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D307	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	
	D308	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D309	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D310	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D311	Tannenbaum, "Computer Networks," pages 202-219 (1996)	
	D312	Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D315	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D317	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D318	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D319	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D320	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D321	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D322	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D323	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D324	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D325	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D326	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent.	
	D327	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D328	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D329	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D330	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D331	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D332	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D333	Exhibit 19, RFC 2595 vs. Claims of the '211 Patent	
	D334	Exhibit 20, RFC 2595 vs. Claims of the '504 Patent	
	D335	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D336	Exhibit 22, iPASS vs. Claims of the '211 Patent	
	D337	Exhibit 23, iPASS vs. Claims of the '504 Patent	
	D338	Exhibit 24, "US '034" vs. Claims of the '135 Patent	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034") vs. Claims of the '211 Patent	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034") vs. Claims of the '504 Patent	
	D341	Exhibit 27, US '287 vs. Claims of the '135 Patent	
	D342	Exhibit 28, US '287 vs. Claims of the '211 Patent	
	D343	Exhibit 29, US '287 vs. Claims of the '504 Patent	
	D344	Exhibit 30, Overview of Access VPNs vs. Claims of the '135 Patent	
	D345	Exhibit 31, Overview of Access VPNs vs. Claims of the '211 Patent	
	D346	Exhibit 32, Overview of Access VPNs vs. Claims of the '504 Patent	
	D347	Exhibit 34, RFC 1928 vs. Claims of the '135 Patent	
	D348	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D349	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D350	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D351	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D352	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D353	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D354	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D355	Exhibit 42,SecureConnect vs. Claims of the '504 Patent	
	D356	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D357	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D358	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D359	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D360	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D361	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D362	Exhibit 49, US '132 vs. Claims of the '135 Patent	
	D363	Exhibit 50, US '132 vs. Claims of the '211 Patent	
	D364	Exhibit 51, US '132 vs. Claims of the '504 Patent	
	D365	Exhibit 52, US '213 vs. Claims of the '135 Patent	
	D366	Exhibit 53, US '213 vs. Claims of the '211 Patent	
	D367	Exhibit 54, US '213 vs. Claims of the '504 Patent	
	D368	Exhibit 55, B&M VPNs vs. Claims of the '135 Patent	
	D369	Exhibit 56, B&M VPNs vs. Claims of the '211 Patent	
	D370	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D371	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D372	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D373	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D374	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D375	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D376	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D377	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D378	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D379	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D380	Exhibit 67, RFC 2486 vs. Claims of the '135 Patent	
	D381	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D382	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D383	Exhibit 70, Understanding IPSec vs. Claims of the '135 Patent	
	D384	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D385	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D386	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D387	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D388	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D389	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D390	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D391	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D392	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D393	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D394	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D395	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D396	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D397	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D398	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D399	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D400	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D401	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D402	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D403	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D404	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D405	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D406	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D407	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D408	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D409	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D410	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D411	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D412	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D413	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D414	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D415	Exhibit 102, NIKKEI vs. Claims of the '211 Patent	
	D416	Exhibit 103, NIKKEI vs. Claims of the '504 Patent	
	D417	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D418	Exhibit 105, Omron vs. Claims of the '135 Patent	
	D419	Exhibit 106, Gauntlet System vs. Claims of the '135 Patent	
	D420	Exhibit 107, Gauntlet System vs. Claims of the '151 Patent	
	D421	Exhibit 108, Gauntlet System vs. Claims of the '180 Patent	
	D422	Exhibit 109, Gauntlet System vs. Claims of the '211 Patent	
	D423	Exhibit 110, Gauntlet System vs. Claims of the '504 Patent	
	D424	Exhibit 111, Gauntlet System vs. Claims of the '759 Patent	
	D425	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D426	Exhibit 113, IntraPort System vs. Claims of the '151 Patent	
	D427	Exhibit 114, IntraPort System vs. Claims of the '180 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D428	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D429	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D430	Exhibit 117, IntraPort System vs. Claims of the '759 Patent	
	D431	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D432	Exhibit 119, Altiga VPN System vs. Claims of the '151 Patent	
	D433	Exhibit 120, Altiga VPN System vs. Claims of the '180 Patent	
	D434	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D435	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D436	Exhibit 123, Altiga VPN System vs. Claims of the '759 Patent	
	D437	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D438	Exhibit 125, Kiuchi vs. Claims of the '151 Patent	
	D439	Exhibit 126, Kiuchi vs. Claims of the '180 Patent	
	D440	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D441	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D442	Exhibit 129, Kiuchi vs. Claims of the '759 Patent	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '151 Patent	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '180 Patent	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D448	Exhibit 135, Overview vs. Claims of the '759 Patent	
	D449	Exhibit 136, RFC 2401 vs. Claims of the '759 Patent	
	D450	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D451	Exhibit 138, Schulzrinne vs. Claims of the '151 Patent	
	D452	Exhibit 139, Schulzrinne vs. Claims of the '180 Patent	
	D453	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D454	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D455	Exhibit 142, Schulzrinne vs. Claims of the '759 Patent	
	D456	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D457	Exhibit 144, Solana vs. Claims of the '151 Patent	
	D458	Exhibit 145, Solana vs. Claims of the '180 Patent	
	D459	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D460	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D461	Exhibit 148, Solana vs. Claims of the '759 Patent	
	D462	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D463	Exhibit 150, Atkinson vs. Claims of the '151 Patent	
	D464	Exhibit 151, Atkinson vs. Claims of the '180 Patent	
	D465	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D466	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D467	Exhibit 154, Atkinson vs. Claims of the '759 Patent	
	D468	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D469	Exhibit 156, Marino vs. Claims of the '151 Patent	
	D470	Exhibit 157, Marino vs. Claims of the '180 Patent	
	D471	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D472	Exhibit 159, Marino vs. Claims of the '504 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known
	Application Number: 95/001,851
	Filing Date: December 13, 2011
	First Named Inventor: Victor Larson
	Art Unit: 3992
	Examiner Name: Roland G. Foster
	Docket Number: 11798.0007-00000

	D473	Exhibit 160, Marino vs. Claims of the '759 Patent	
	D474	Exhibit 161, Aziz ('646) vs. Claims of the '759 Patent	
	D475	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D476	Exhibit 163, Wesinger vs. Claims of the '151 Patent	
	D477	Exhibit 164, Wesinger vs. Claims of the '180 Patent	
	D478	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D479	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D480	Exhibit 167, Wesinger vs. Claims of the '759 Patent	
	D481	Exhibit 168, Aziz ('234) vs. Claims of the '135 Patent	
	D482	Exhibit 169, Aziz ('234) vs. Claims of the '151 Patent	
	D483	Exhibit 170, Aziz ('234) vs. Claims of the '180 Patent	
	D484	Exhibit 171, Aziz ('234) vs. Claims of the '211 Patent	
	D485	Exhibit 172, Aziz ('234) vs. Claims of the '504 Patent	
	D486	Exhibit 173, Aziz ('234) vs. Claims of the '759 Patent	
	D487	Exhibit 174, Schneider vs. Claims of the '759 Patent	
	D488	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D489	Exhibit 176, Valencia vs. Claims of the '151 Patent	
	D490	Exhibit 177, Valencia vs. Claims of the '180 Patent	
	D491	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D492	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867 vs. Claims of the '180 Patent	
	D494	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D495	Exhibit 182, Davison vs. Claims of the '151 Patent	
	D496	Exhibit 183, Davison vs. Claims of the '180 Patent	
	D497	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D498	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D499	Exhibit 186, Davison vs. Claims of the '759 Patent	
	D500	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D501	Exhibit 188, AutoSOCKS v2.1 vs. Claims of the '151 Patent	
	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide vs. Claims of the '180 Patent	
	D503	Exhibit 190, AutoSOCKS vs. Claims of the '759 Patent	
	D504	Exhibit 191, Aventail Connect 3.01/2.51 vs. Claims of the '135 Patent	
	D505	Exhibit 192, Aventail Connect v3.01/2.51 vs. Claims of the '151 Patent	
	D506	Exhibit 193, Aventail Connect 3.01/2.51 vs. Claims of the '180 Patent	
	D507	Exhibit 194, Aventail Connect 3.01/2.51 vs. Claims of the '759 Patent	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '135 Patent	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '151 Patent	
	D510	Exhibit 197, Aventail Connect 3.1/2.6 vs. Claims of the '180 Patent	
	D511	Exhibit 198, Aventail Connect 3.1/2.6 vs. Claims of the '759 Patent	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '151 Patent	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 Patent	
	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D517	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D518	Exhibit 205, Domain Name System (DNS) Security vs. Claims of the '504 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO	Complete if Known
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number: 95/001,851
	Filing Date: December 13, 2011
	First Named Inventor: Victor Larson
	Art Unit: 3992
	Examiner Name: Roland G. Foster
	Docket Number: 11798.0007-00000

	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '135 Patent	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '151 Patent	
	D528	Exhibit 215, U.S. Patent No. 6,643,701 vs. Claims of the '135 Patent	
	D529	Exhibit 216, U.S. Patent No. 6,643,701 vs. Claims of the '151 Patent	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '151 Patent	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '135 Patent	
	D532	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D533	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '151 Patent	
	D535	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D536	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '151 Patent	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System vs. Claims of the '759 Patent	
	D546	Exhibit A: Copy of U.S. Patent No. 6,502,135	
	D547	Exhibit A: Copy of U.S. Patent No. 7,490,151	
	D548	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D549	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D550	Exhibit B-1: File History of U.S. Patent 6,502,135	
	D551	Exhibit B-2: Reexamination Record No. 95/001,269	
	D552	Exhibit C1: Claim Chart – Aventail Connect v3.1 (Patent No. 6,502,135)	
	D553	Exhibit C2: Claim Chart Aventail Connect V3.01 (Patent No. 6,502,135)	
	D554	Exhibit C-1: Copy of U.S. Patent No. 7,010,604	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D555	Exhibit C2: Claim Chart Aventail Autosocks (Patent No. 7,490,151)	
	D556	Exhibit C1: Claim Chart Aventail Connect v3.01 (Patent No. 7,490,151)	
	D557	Exhibit C-2: Provisional Application 60/106,261	
	D558	Exhibit C3: Claim Chart Aventail AutoSOCKS (Patent No. 6,502,135)	
	D559	Exhibit C3: Claim Chart BinGO (Patent No. 7,490,151)	
	D560	Exhibit C-3: Provisional Application 60/137,704	
	D561	Exhibit C4: Claim Chart Wang (Patent No. 6,502,135)	
	D562	Exhibit C4: Claim Chart Beser (Patent No. 7,490,151)	
	D563	Exhibit C5: Claim Chart Beser (Patent No. 6,502,135)	
	D564	Exhibit C5: Claim Chart Wang (Patent No. 7,490,151)	
	D565	Exhibit C6: Claim Chart BinGO (Patent No. 6,502,135)	
	D566	Exhibit D: Memorandum Opinion in *VirnetX v. Microsoft.*	
	D567	Exhibit D-1: Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HPPT-Based Network on the Internet," Published in the Proceedings of SNDSS 1996.	
	D568	Exhibit D-10: D.E. Denning and G.M. Sacco, "Time-stamps in Key Distribution Protocols," Communications of the ACM, Vol. 24, N.8, pp. 533-536. August 1981.	
	D569	Exhibit D-11: C.I. Dalton and J.F. Griffin, "Applying Military Grade Security to the Internet," Proceedings of the 8th Joint European Networking Conference (JENC 8), (May 12-15 1997).	
	D570	Exhibit D-12: Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based protocols Secure against Dictionary Attacks," 1992 IEEE Symposium on Security and Privacy (1992).	
	D571	Exhibit D-2: Copy of U.S. Pat. No. 5,898,830	
	D572	Exhibit D-3: Eduardo Solana and Jürgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains,", Security Protocols Workshop 1997, pp. 37-51.	
	D573	Exhibit D-4: Copy of U.S. Pat. No. 6,119,234	
	D574	Exhibit D-5: Jeff Sedayao, "'Mosaic Will Kill My Network!' – Studying Network Traffic Patterns of Mosaic Use," in Electron. Proc. 2nd World Wide Web Conf.'94: Mosaic and the Web, Chicago, IL, Oct. 1994.	
	D575	Exhibit D-6: M. Luby Juels and R. Ostrovsky, "Security of Blind Digital Signatures," Crypto '97, LNCS 1294, pages 150-164, Springer-Verlag, Berlin, 1997.	
	D576	Exhibit D-8: David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).	
	D577	Exhibit D-9: Copy of U.S. Pat. No. 7,764,231	
	D578	Exhibit E-1: Claim Charts Applying Kiuchi and Other References to Claims of the '135 Patent.	
	D579	Exhibit E1: Declaration of Chris Hopen (Patent No. 6,502,135)	
	D580	Exhibit E1: Declaration of Chris Hopen (Patent No. 7,490,151)	
	D581	Exhibit E-2: Claim Charts Applying Wesinger and Other References to Claims of the '135 Patent.	
	D582	Exhibit E2: Declaration of Michael Fratto (Patent No. 6,502,135)	
	D583	Exhibit E2: Declaration of Michael Fratto (Patent No. 7,490,151)	
	D584	Exhibit E-3: Claim Charts Applying Solana and Other References to Claims of the '135 Patent.	
	D585	Exhibit E3: Declaration of James Chester (Patent No. 6,502,135)	
	D586	Exhibit E3: Declaration of James Chester (Patent No. 7,490,151)	
	D587	Exhibit E-4: Claim Charts Applying Aziz and Other References to Claims of the '135 Patent.	
	D588	Exhibit X1: Aventail Connect Administrator's Guide v3.1/v2.6., PP 1-20 (1996-1999)	
	D589	Exhibit X10: Copy of U.S. Patent No. 4,885,778	
	D590	Exhibit X11: Copy of U.S. Patent No. 6,615,357	
	D591	Exhibit X2: Aventail Connect Administrator's Guide v3.01/v2.51., PP 1-116 (1996-1999)	
	D592	Exhibit X3: Aventail AutoSOCKS Administration & User's Guide v2.1., PP 1-70 (1996-1999)	
	D593	Exhibit X4: Reed et al., "Proxies for Anonymous Routine," 12th Annuary Computer Security Applications Conference, San Diego, CA, December -9-13, pp 1-10 (1996).	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D594	Exhibit X5: Wang, The Broadband Forum Technical Report, "TR-025 – Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL," Issue 1.0; pp. 1-24 , v1.0 (1999).	
	D595	Exhibit X6: Copy of U.S. Patent No. 6,496,867	
	D596	Exhibit X7: BinGO! User's Guide Incorporating by Reference BinGO! Extended Feature Reference.	
	D597	Exhibit X7: Kent et al., "Security Architecture for the Internet Protocol, " Network Working Group Request for Comments (RFC) 2401, pp 1-70 (1998).	
	D598	Exhibit X8: Copy of U.S. Patent No. 6,182,141	
	D599	Exhibit X9: BinGO! User's Guide v1.6 (1999).	
	D600	Exhibit Y1: Aventail Extranet Server 3.0 Administrator's Guide.	
	D601	Exhibit Y10: Hanks, S., et al., RFC1701, "Generic Routing Encapsulation (GRE)," 1994, Is Accessbile at http://www.ietf.org/rfc/rfc1701.txt.	
	D602	Exhibit Y10: Socolofsky, T. et al., RFC 1180, "A TCP/IP Tutorial," January 1991.	
	D603	Exhibit Y11: Simpson, W., editor, RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994.	
	D604	Exhibit Y11: Simpson, W., RFC1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," 1996, http://www.ietf.org/rdc/rfc1994.txt.	
	D605	Exhibit Y12: Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996.	
	D606	Exhibit Y12: Perkins, D., RFC1171, "The Point-To-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-To-Point Links," 1990, Is Accessible at http://www.ietf.org/rfc/rfc1171.txt.	
	D607	Exhibit Y13: Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September, 1998.	
	D608	Exhibit Y14: Townsley, W.M., et al., RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999.	
	D609	Exhibit Y15: Pall, G.S., RFC 2118, "Microsoft Point-To-Point Encryption (MPPE) Protocol," March 1997.	
	D610	Exhibit Y16: Gross, G., et al., RFC 2364, "PPP Over AAL5," July 1998.	
	D611	Exhibit Y17: Srisuresh, P., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999.	
	D612	Exhibit Y18: Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993.	
	D613	Exhibit Y2: Goldschlag et al., "Hiding Routing Information" (1996).	
	D614	Exhibit Y3: Copy of U.S. Patent No. 5,950,519	
	D615	Exhibit Y4: Ferguson, P. and Huston, G., "What Is a VPN", The Internet Protocol Journal, Vol 1., No. 1 (June 1998 ("Ferguson").	
	D616	Exhibit Y5: Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC1034").	
	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodburn, R.A., et al., RFC1241, "A Scheme for an Internet Encapsulation Protocol: Version 1," 1991.	
	D620	Exhibit Y9: Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996.	
	D621	Exhibit Y9: Simpson, W., RFC1853, "IP in IP Tunneling," 1995, Is Accessible at http://ww.ietf.org/rfc/rfc1583.txt.	
	D622	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 6,502,135)	
	D623	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 7,490,151)	
	D624	Request for Inter Partes Reexamination (Patent No. 6,502,135)	
	D625	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 6,502,135)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

	D626	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 7,490,151)	
	D627	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D628	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D629	Transmittal Letter (Patent No. 6,502,135)	
	D630	Transmittal Letter (Patent No. 7,490,151)	
	D631	Joint Claim Construction and Prehearing Statement	
	D632	Exhibit A: Agreed Upon Terms; P.R. 4-3 Joint Claims Construction and Prehearing Statement	
	D633	Exhibit B: Disputed Claim Terms; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D634	Exhibit C; VirnetX's Proposed Construction of Claim Terms and Supporting Evidence	
	D635	Exhibit D; Defendants' Intrinsic and Extrinsic Support; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D636	U.S. Patent 6,839,759	
	D637	Exhibit B-4; VirnetX, Inc. v. Microsoft Corp., Case No. 6:07-cv-80, Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759 (E.D. Tex. Dec. 18, 2009)	
	D638	Exhibit D-2; Kent et al., "Security Architecture for the Internet Protocol," Internet Engineering Task Force, Internet Draft, (Feb. 1998)	
	D639	Exhibit D-3; Aziz et al., U.S. Patent 5,548,646 to Aziz et al., "System for Signatureless Transmission and Reception of Data Packets Between Computer Networks," Filed Sept. 15, 1994 and issued Aug. 20, 1996	
	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Internet Protocol," DARPA Internet Program Specification RFC 791 (Sept. 1981)	
	D644	Exhibit D-14; Caronni et al., "SKIP – Securing the Internet," 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '96) (June 19-21, 1996)	
	D645	Exhibit D-15; Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP), " IPSEC Work Group Draft (July 26, 1997)	
	D646	Exhibit E-1; Claim Charts Applying Kiuchi as a Primary Reference to the '759 Patent.	
	D647	Exhibit E-2; Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D648	Exhibit E-3; Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D649	Exhibit E-4; Claim Charts Applying Kent in view of Caronni as a Primary Combination of References to the '759 Patent	
	D650	Exhibit D-5; Edwards et al., "High Security Web Servers and Gateways," Computer Networks and ISDN System 29, pages 927-938 (Sept. 1997)	
	D651	Exhibit D-10; Lee et al., "Hypertext Transfer Protocol – HTTP/1.0," RFC 1945 (May 1996)	
	D652	Exhibit E-3; Claim Charts Applying Blum to Claims of the '151 Patent	
	D653	Exhibit B-1, File History of U.S. Patent 7,490,151	
	D654	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D655	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D656	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D657	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D658	VirnetX Inc., V. Mitel Networks Corp.; Defendants' Joint Invalidity Contentions	
	D659	Exhibit 37, REC 2661 vs. Claims of the '135 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known
	Application Number: 95/001,851
	Filing Date: December 13, 2011
	First Named Inventor: Victor Larson
	Art Unit: 3992
	Examiner Name: Roland G. Foster
	Docket Number: 11798.0007-00000

	D660	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D661	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D662	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D663	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D664	Exhibit 42, SecureConnect vs. Claims of the '504 Patent	
	D665	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D666	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D667	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D668	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D669	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D670	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D671	Exhibit 49, Chuah vs. Claims of the '135 Patent	
	D672	Exhibit 50, Chuah vs. Claims of the '211 Patent	
	D673	Exhibit 51, Chuah vs. Claims of the '504 Patent	
	D674	Exhibit 52, U.S. '648 vs. Claims of the '135 Patent	
	D675	Exhibit 53, U.S. '648 vs. Claims of the '211 Patent	
	D676	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D677	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D678	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D679	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D680	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D681	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D682	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D683	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D684	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D685	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D686	Exhibit 67, US '072 vs. Claims of the '135 Patent	
	D687	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D688	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D689	Exhibit 70 Understanding IPSec vs. Claims of the '135 Patent	
	D690	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D691	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D692	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D693	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D694	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D695	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D696	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D697	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D698	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D699	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D700	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D701	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D702	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D703	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D704	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D705	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D706	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D707	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D708	Exhibit 89, US '671 vs. Claims of the '211 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D709	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D710	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D711	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D712	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D713	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D714	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D715	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D716	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D717	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D718	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D719	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D720	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D721	Exhibit 102, Nikkei vs. Claims of the '211 Patent	
	D722	Exhibit 103, Nikkei vs. Claims of the '504 Patent	
	D723	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D724	Exhibit 106-A, Gauntlet System vs. Claims of the '135 Patent	
	D725	Exhibit 109-A, Gauntlet System vs. Claims of the '211 Patent	
	D726	Exhibit 110-A, Gauntlet System vs. Claims of the '504 Patent	
	D727	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D728	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D729	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D730	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D731	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D732	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D733	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D734	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D735	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D736	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D737	Exhibit 137, Schulzrinne vs. Claims of the '135 (Final) Patent	
	D738	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D739	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D740	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D741	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D742	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D743	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D744	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D745	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D746	Exhibit 168, Aziz vs. Claims of the '135 Patent	
	D747	Exhibit 171, U.S. '234 vs. Claims of the '211 Patent	
	D748	Exhibit 172, Aziz vs. Claims of the '504 Patent	
	D749	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D750	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D751	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D752	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D753	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D754	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP' vs. Claims of the '135 Patent	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401' vs. Claims of the '135 Patent	
	D763	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D764	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D765	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D766	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D768	Exhibit 228, U.S. 588 vs. Claims of the '211 Patent (Final)	
	D769	Exhibit 229, U.S. 588 vs. Claims of the '504 Patent (Final)	
	D770	Exhibit 230, Microsoft VPN vs. Claims of the '135 Patent (Final)	
	D771	Exhibit 231, Microsoft VPN vs. Claims of the '211 Patent (Final)	
	D772	Exhibit XX, Microsoft VPN vs. Claims of the '504 Patent	
	D773	Exhibit Cisco-1, Cisco's Prior Art System vs. Claims of the '135 Patent	
	D774	Exhibit Cisco-4, Cisco's Prior Art System vs. Claims of the '211 Patent	
	D775	Exhibit Cisco-5, Cisco's Prior Art System vs. Claims of the '504 Patent	
	D776	Exhibit 225, US '037 vs. Claims of the '135 Patent	
	D777	Exhibit 226, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D778	Exhibit 227, US '393 vs. Claims of the '135 Patent	
	D779	Exhibit 233, The Miller Application vs. Claim 13 of the '135 Patent	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '504 Patent	
	D781	Exhibit 235, Microsoft VPN vs. Claims of the '504 Patent	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '211 Patent	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '504 Patent	
	D784	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D785	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D786	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D787	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D788	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D789	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D790	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D791	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D792	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D793	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent	
	D794	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D795	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D796	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D797	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known
	Application Number: 95/001,851
	Filing Date: December 13, 2011
	First Named Inventor: Victor Larson
	Art Unit: 3992
	Examiner Name: Roland G. Foster
	Docket Number: 11798.0007-00000

	D798	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D799	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D800	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D801	Exhibit 22, iPass vs. Claims of the '211 Patent	
	D802	Exhibit 23, iPass vs. Claims of the '504 Patent	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 135 Patent	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 211 Patent	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 504 Patent	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 135 Patent	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 211 Patent	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 504 Patent	
	D809	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D810	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D811	Exhibit 106, Gaunlet System and Gaunlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gaunlet System and Gaunlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gaunlet System vs. Claims of the '504 Patent	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D817	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D818	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D819	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D820	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D821	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D822	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D823	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect") vs. Claims of the '135 Patent	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '135 Patent	
	D826	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D827	Exhibit 205, Domain Name System (DNS) Security ("DNS Security") vs. Claims of the '504 Patent	
	D828	Exhibit 210, Lendenmann vs. Claims of the '211 Patent	
	D829	Exhibit 211, Lendenmann vs. Claims of the '504 Patent	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D831	Exhibit 215, Aziz vs. Claims of the '135 Patent	
	D832	Cisco '180, Efiling Acknowledgment	
	D833	Exhibit A, U.S. Patent 7,188,180	
	D834	Exhibit B1, File History of U.S. Patent 7,188,180	
	D835	Exhibit B2, File History of U.S. Patent Application No. 09/588,209	
	D836	Exhibit B3, File History of Reexamination Control No. 95/001,270, Reexamination of U.S. 7,188,180 requested by Microsoft Corp	
	D837	Exhibit D1, "Lendenmann": Rolf Lendenman, Understanding OSF DCE 1.1 For AIX and OS/2, IBM International Technical Support Organization (Oct. 1995).	
	D838	Exhibit D5, "Schneier": Bruce Schneier, Applied Cryptography (1996)	
	D839	Exhibit D6, RFC 793; Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Specification RFC 793 (Sept. 1981)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO	Complete if Known	95001851 - GAU: 3992
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	
	D841	Exhibit D8, "Rosenberry"; Ward Rosenberry, David Kenney, and Gerry Fisher, Understanding DCE (1993)	
	D842	Exhibit D9, Masys; Daniel R. Masys & Dixie B. Baker, "Protecting Clinical Data on Web Client Computers: The PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, Florida (Nov. 7-11, 1998)	
	D843	Exhibit E1, Claim Charts Applying Lendenmann as a Primary Reference to the '180 Patent.	
	D844	Exhibit E2, Claim Charts Applying Kiuchi as a Primary Reference to the '180 Patent	
	D845	Exhibit E3, Claim Charts Applying Solana as a Primary Reference to the '180 Patent	
	D846	Exhibit E4, Claim Charts Applying Schimpf and Rosenberry as a Primary Reference to the '180 Patent	
	D847	Request for Inter Partes Reexamination of Patent No. 7,188,180	
	D848	Modified PTO Form 1449	
	D849	Request for Inter Partes Reexamination Transmittal Form No. 7,188,180	
	D850	Exhibit A; U.S. Patent 7,921,211 with Terminal Disclaimer	
	D851	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,921,211)	
	D852	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D853	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D854	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser)	
	D855	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D856	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D857	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D858	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D859	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D860	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D861	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D862	Exhibit X1, Solana, E. et al. "Flexible Internet Secure Transactions Based on Collaborative Domains"	
	D863	Exhibit X2, U.S. Patent 6,557,037	
	D864	Exhibit X4, Atkinson, R., IETF RFC 2230, "Key Exchange Delegation Record for the DNS" (November 1997)	
	D865	Exhibit X6, Kent, et al., IETF RFC 2401, "Security Architecture for the Internet Protocol" (November 1998) Is Accessible at: http://www.ietf.org/rfc/rfc2401.txt	
	D866	Exhibit X7, Eastlake, D. et al., IETF RFC 2065, "Domain Name System Security Extensions" (January 1997) Is Accessible at: http://www.ietf.org/rfc/rfc2065.txt	
	D867	Exhibit X9, Guttman, E. et al., IETF RFC 2504, "Users' Security Handbook" (February 1999) Is Accessible At: http://www.ietf.org/rfc/rfc2504.txt	
	D868	Exhibit Y3, Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989 ("RFC1123").	
	D869	Exhibit Y4, Atkinson, R., RFC 1825, "Security Architecture for the Internet Protocol (August 1995) Is Accessible At: http://www.ietf.org/rfc/rfc1825.txt	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Sheet 1 of 4				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**95/001,851**
				Filing Date	**December 13, 2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**3992**
				Examiner Name	**Roland G. Foster**
				Docket Number	**11798.0007-00000**

	D870	Exhibit Y5, Housley, R. et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (January 1999) Is accessible At: http://www.ietf.org/rfc/rfc2459.txt	
	D871	Exhibit A, U.S. Patent 7,418,504	
	D872	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,418,504)	
	D873	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D874	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in view of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D875	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D876	Exhibit C4, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D877	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed, and Beser	
	D878	Exhibit C6, Claim Chart – USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D879	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D880	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D881	Exhibit D1, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act. 6:2010cv00417 (E.D. Tex)	
	D882	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. against Apple Inc. Based on the 7,418,504	
	D883	Exhibit X5, Eastlake, D., et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)" (March 1999)	
	D884	Exhibit X6, Kent, S. IETF RFC 2401, "Security Architecture for the Internet Protocol, (November1998) http://www.ietf.org/rfc/rfc2401.txt	
	D885	Exhibit X8, Postel, J. et al., IETF RFC 920, "Domain Requirements" (October 1984) Is Accessible at http://www.ietf.org/rfc/rfc920.txt	
	D886	Exhibit X10, Reed, M. et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996.	
	D887	Request for Inter Partes Reexamination Transmittal form	
	D888	Transmittal Letter	
	D889	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D890	Exhibit D-7, "Thomas": Brian Thomas, "Recipe for E-Commerce, IEEE Internet Computing, (Nov.-Dec. 1997)	
	D891	Exhibit D-9, "Kent II": Stephen Kent & Randall Atkinson, "IP Encapsulating Security Payload (ESP)," Internet Engineering Task Force, Internet Draft (Feb. 1998)	
	D892	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser (Came from Inval. Cisco dtd 11/18/11)	
	D893	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D894	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D895	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D896	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D897	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)	Complete if Known	
	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D898	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D899	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D900	211 Request for Inter Partes Reexamination	
	D901	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D902	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D903	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D904	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D905	Exhibit C6, USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D906	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D907	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D908	504 Request for Inter Partes Reexamination	
	D909	Defendants' Supplemental Joint Invalidity Contentions	
	D910	Exhibit 226, Securing Web Access with DCE vs. Claims of the '135 Patent	
	D911	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D918	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D921	Exhibit 237, U.S. '648 vs. Claims of the '135 Patent	
	D922	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D923	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D924	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D925	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D926	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D927	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D928	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D929	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D930	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D931	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D932	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D933	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D934	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D936	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D937	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D938	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	D939	Exhibit A, Aventail Press Release, May 2, 1997	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D940	Exhibit B, InfoWorld, "Aventail Delivers Highly Secure, Flexible VPN Solution," InfoWorld, page 64D, (1997)	
	D941	Exhibit C, Aventail AutoSOCKS v2.1 Administrator's Guide	
	D942	Exhibit D, Aventail Press Release, October 12, 1998	
	D943	Exhibit G, Aventail Press Release, May 26, 1999	
	D944	Exhibit H, Aventail Press Release, August 9, 1999	
	D945	Exhibit J, "Aventail ExtraNet Center 3.1: Security with Solid Management, Network Computing, June 28, 1999	
	D946	Petition in Opposition to Patent Owner's Petition to Vacate Inter Partes ReExamination Determination on Certain Prior Art	
	D947	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D948	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under U.S.C. § 311	
	D949	Exhibit C1, Claim Chart Aventail Connect v3.1	
	D950	Exhibit C2, Claim Chart Aventail Connect v3.01	
	D951	Exhibit C3, Claim Chart Aventail AutoSOCKS	
	D952	Exhibit C4, Claim Chart Wang	
	D953	Exhibit C5, Claim Chart Beser	
	D954	Exhibit C6, Claim Chart BINGO	
	D955	Exhibit X6, U.S. Patent 6,496,867	
	D956	Exhibit X10, U.S. Patent 4,885,778	
	D957	Exhibit X11, U.S. Patent 6,615,357	
	D958	Exhibit Y3, U.S. Patent 5,950,519	
	D959	Request for Inter Partes Reexamination Transmittal Form	
	D960	Transmittal Letter	
	D961	Exhibit D, v3.1 Administrator's Guide	
	D962	Exhibit E-1, Claim Charts Applying Kiuchi to Various Claims of the '135 Patent	
	D963	Exhibit E-2, Claim Charts Applying Wesinger to Various Claims of the '135 Patent	
	D964	Exhibit E-3, Claim Charts Applying Solana to Various Claims of the '135 Patent	
	D965	Exhibit E-4, Claim Charts Applying Aziz to Various Claims of the '135 Patent	
	D966	Request for Inter Partes Reexamination Transmittal Form	
	D967	Request for Inter Partes Reexamination	
	D968	PTO Form 1449	
	D969	Exhibit C1, Claim Chart Aventail Connect v3.01	
	D970	Exhibit C2, Claim Chart Aventail AutoSOCKS	
	D971	Exhibit C3, Claim Chart BINGO	
	D972	Exhibit C4, Claim Chart Beser	
	D973	Exhibit C5, Claim Chart Wang	
	D974	Transmittal Letter	
	D975	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D976	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D977	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D978	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D979	Exhibit E-3, Claim Charts Applying Blum to Claims of the '151 Patent	
	D980	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D981	Exhibit E-5, Claim Charts Applying Kiuchi and Edwards, and Kiuchi, Edwards, and Martin to Claims of the '151 Patent	
	D982	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D983	Exhibit A, U.S. Patent 6,839,759	
	D984	Exhibit C-1, U.S. Patent 6,502,135	
	D985	Exhibit E-1, Claim Charts Applying Kiuchi, as Primary Reference to the '759 Patent	
	D986	Exhibit E-2, Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D987	Exhibit E-3, Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D988	Exhibit E-4, Claim Charts Applying Kent in View of Caronni as a Primary Combination of References to the '759 Patent	
	D989	Request for Inter Partes Reexamination Transmittal Form	
	D990	Request for Inter Partes Reexamination	
	D991	PTO Form 1449	
	D992	Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D993	Request for Inter Partes Reexamination	
	D994	Request for Inter Partes Reexamination Transmittal Form	
	D995	Request for Inter Partes Reexamination	
	D996	Request for Inter Partes Reexamination Transmittal Form	
	D997	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D998	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D999	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D1000	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D1001	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D1002	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D1003	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1004	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1005	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D1006	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D1007	Exhibit B1, File History of U.S. Patent 7,418,504	
	D1008	Exhibit B2, File History of U.S. Patent Application No. 09/558,210	
	D1009	Exhibit D-10, Gaspoz et al., "VPN on DCE: From Reference Configuration to Implementation," Bringing Telecommunication Services to the People – IS&N '95, Third International Conference on Intelligence in Broadband Services and Networks, October 1995 Proceedings, Lecture Notes in Computer Science, Vol. 998 (Springer, 1995)	
	D1010	Exhibit D-11, Copy of U.S. Patent No. 6,269,099	
	D1011	Exhibit D-11, Copy of U.S. Patent No. 6,560,634	
	D1012	Exhibit D-13, Pallen, "The World Wide Web," British Medical Journal, Vol. 311 at 1554 (Dec. 1995)	
	D1013	Exhibit D-14, Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21:120-126 (Feb. 1978)	
	D1014	Exhibit D-15, Copy of U.S. Patent No. 4,952,930	
	D1015	Exhibit D-17, Pfaffenberger, Netscape Navigator 3.0: Surfing the Web and Exploring the Internet, Academic Press (1996)	
	D1016	Exhibit D-18, Gittler et al., "The DCE Security Service," Hewlett-Packard Journal, pages 41-48 (Dec. 1995)	
	D1017	Exhibit D-6, Copy of U.S. Patent No. 5,689,641	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,851
Filing Date	December 13, 2011
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Roland G. Foster
Docket Number	11798.0007-00000

	D1018	Exhibit D-9, Lawton, "New Top-Level Domains Promise Descriptive Names," Sunworld Online, 1996	
	D1019	Exhibit E-1, Copy of Catalog Listing by IBM for RS/6000 Redbooks Collection which includes a Link to the *Lendenmann* reference. The link to the *Lendenmann* reference was archived at archive.org on December 7, 1998 and retrieved by the Wayback Machine	
	D1020	Exhibit E-10, copy of an Archived Version of the Lawton reference archived at archive.org on February 19, 1999 and retrieved by the Wayback Machine	
	D1021	Exhibit E-11, Abstracts of the Proceedings of the Symposium on Network and Distributed System Security, 1996, Archived at archive.org on April 10, 1997, and retrieved by the Wayback Machine	
	D1022	Exhibit E-12, 1996 Symposium on Network and Distributed System Security, Website Archived by archive.org (Apr. 10, 1997), Retrieved by the Wayback Machine at http://web.archive.org/web/19970410114853/http://computer.org/cspress/catalog/proc9.htm.	
	D1023	Exhibit E-13, Copy of Search Results for ISBN 0-12-553153-2 (Pfaffenberger) from www.isbnsearch.org	
	D1024	Exhibit F-1, Claim Charts applying Lendenmann as a Primary Reference to the '504 Patent.	
	D1025	Exhibit F-2, Claim Charts applying Aziz as a Primary Reference to the '504 Patent	
	D1026	Exhibit F-3, Claim Charts applying Kiuchi and Pfaffenberger as Primary References to the '504 Patent	
	D1027	Exhibit E-2, First Page of U.S. Patent No. 5,913,217 published June 15, 1999 and citing a portion of the Lendenmann reference as a prior art reference	
	D1028	Exhibit E-3, Request for Comments 2026, "The Internet Standards Process – Revision 3," October 1996	
	D1029	Exhibit E-4, First Page of U.S. 5,463,735, published October 31, 1995 and citing RFC 793 as a prior art Reference	
	D1030	Exhibit E-5, Copy of catalog listing from Boston University Digital Common Website, listing the Martin reference with an issue date of February 21, 1998	
	D1031	Exhibit E-6, Copy of Technical Reports Archive Listing from Boston University Computer Science Department which includes a link to the Martin paper. The link to the Martin paper was archived at archive.org on January 22, 1998 and Retrieved by the Wayback Machine	
	D1032	Exhibit E-7, Boston University Computer Science Department Technical Reports Instructions, available at: http://www.cs.bu.edu/techreports/INSTRUCTIONS	
	D1033	Exhibit E-8, U. Möller, "Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe," Diplomarbeit, Universität Hamburg (July 16, 1999), citing to Martin at page 77.	
	D1034	Exhibit E-9, First page of U.S. 5,737,423, published April 7, 1998 and citing Schneier as Prior Art Reference	
	D1035	Request for Inter Partes ReExamination; U.S. Patent 7,418,504	
	D1036	Request for Inter Partes ReExamination Transmittal Form; U.S. Patent 7,418,504	
	D1037	PTO Form 1449	
	D1038	Exhibit C1, Claim Chart – USP 7,921,211 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1039	Exhibit C2, Claim Chart – USP 7,921,211 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1040	Exhibit C3, Claim Chart – USP 7,921,211 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1041	Exhibit C4, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2230 and further in conjunction with RFC 920, Reed and Beser	
	D1042	Exhibit C5, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1043	Exhibit C6, Claim Chart – USP 7,921,211relative to Beser, Alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1044	Exhibit C7, Claim Chart – USP 7,921,211 relative to RFC 2230, alone and in conjunction with RFC 2401, Reed, and Beser	
	D1045	Exhibit C8, Claim Chart – USP 7,921,211 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Receipt date: 04/25/2012

Substitute for form 1449/PTO	Complete if Known	95001851 - GAU: 3992
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

	D1046	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1047	Exhibit C1, Claim Chart – USP 7,418,504 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1048	Exhibit C2, Claim Chart – USP 7,418,504 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1049	Exhibit C3, Claim Chart – USP 7,418,504 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1050	Exhibit C5, Claim Chart – USP 7,418,504 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1051	Exhibit C6, USP 7,418,504 relative to Beser, alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1052	Exhibit C7, Claim Chart – USP 7,418,504 relative to RFC 2230, alone and in conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1053	Exhibit C8, Claim Chart – USP 7,418,504 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1054	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1055	Exhibit 226, Securing Web Access with DCE vs. Claims of the '135 Patent	
	D1056	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D1063	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D1064	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D1065	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D1066	Exhibit 237, U.S. '072 vs. Claims of the '135 Patent	
	D1067	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D1068	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D1069	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D1070	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D1071	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D1072	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D1073	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D1074	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D1075	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D1076	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D1077	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D1078	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D1079	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D1081	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D1083	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	D1084	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1087	Exhibit B1, File History of U.S. Patent 7,921,211	
	D1088	Exhibit B2, File History of U.S. Patent Application No. 10/714,849	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

				Complete if Known	95001851 - GAU: 3992
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**95/001,851**
				Filing Date	**December 13, 2011**
				First Named Inventor	**Victor Larson**
				Art Unit	**3992**
				Examiner Name	**Roland G. Foster**
				Docket Number	**11798.0007-00000**

	D1089	Exhibit B4, *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009)	
	D1090	Exhibit D15, U.S. Patent 4,952,930	
	D1091	Exhibit F1, Claim Charts Applying Lendenmann as a Primary Reference to the '211 Patent	
	D1092	Exhibit F2, Claim Charts Applying Aziz as a Primary Reference to the '211 Patent	
	D1093	Exhibit F3, Claim Charts Applying Kiuchi and Pfaffenberger as Primary References to the '211 Patent	
	D1094	Exhibit 2, Letter and attachment from Ramzi Khazen, Counsel for VirnetX, to Dmitriy Kheyfits, Counsel for Cisco Systems (June 23, 2011)	
	D1095	Exhibit P, Malkin, "Dial-In Virtual Private Networks Using Layer 3 Tunneling"	
	D1096	Exhibit Q, Ortiz, "Virtual Private Networks: Leveraging the Internet"	
	D1097	Exhibit R, Keromytix, "Creating Efficient Fail-Stop Cryptographic Protocols"	
	D1098	Transcript of Markman Hearing Dated January 5, 2012	
	D1099	Declaration of John P. J. Kelly, Ph.D	
	D1100	Defendants' Responsive Claim Construction Brief; Exhibits A–P and 1-7	
	D1101	Joint Claim Construction and Prehearing Statement Dated 11/08/11	
	D1102	Exhibit A: Agreed Upon Terms Dated 11/08/11	
	D1103	Exhibit B: Disputed Claim Terms Dated 11/08/11	
	D1104	Exhibit C: VirnetX's Proposed Construction of Claim Terms and Supporting Evidence Dated 11/08/11	
	D1105	Exhibit D: Defendant's Intrinsic and Extrinsic Support Dated 11/08/11	
	D1106	Declaration of Austin Curry in Support of VirnetX Inc.'s Opening Claim Construction Brief	
	D1107	Declaration of Mark T. Jones Opening Claims Construction Brief	
	D1108	VirnetX Opening Claim Construction Brief	
	D1109	VirnetX Reply Claim Construction Brief	
	D1110	European Search Report from corresponding EP Application Number 11005789 (Our Ref.: 077580-0142)	
	D1111	European Search Report from corresponding EP Application Number 11005792 (Our Ref.: 077580-0143)	
	D1112	ITU-T Recommendation H.323, "Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System," International Telecommunications Union, pages 1-128, February 1998	
	D1113	ITU-T Recommendation H.225.0, "Infrastructure of Audiovisual Services – Transmission Multiplexing and Synchronization. Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication systems," International Telecommunication Union, pages 1-155, February 1998	
	D1114	ITU-T Recommendation H.235, "Infrastructure of Audiovisual Services – Systems Aspects. Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals," International Telecommunication Union, pages 1-39, February 1998	
	D1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	D1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	D1117	Transmittal Letters (Patent No.8,051,181)	
	D1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	

/Roland Foster/ 09/27/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Receipt date: 04/25/2012 95001851 - GAU: 3992

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,851
	Filing Date	December 13, 2011
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Roland G. Foster
	Docket Number	11798.0007-00000

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24, and D257, D258, D259, D261, D263, D264, D266, and D292-D1118).**

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge any required fees to Deposit Account 06-0916.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

/Joseph E. Palys/ Date: April 25, 2012

Joseph E. Palys
Reg. No.: 46,508
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.
901 New York Ave NW
Washington, DC 20001-4413
Tel. (202) 408-4000
Fax (404) 408-4400

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /R.F./

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95001851	7418504
	Certificate Date	Certificate Number

Requester Correspondence Address:	☐ Patent Owner	☒ Third Party

David L. McCombs
HAYNES AND BOONE, LLP, IP SECTION
2323 Victory Avenue, Suite 700
Dallas, TX 75219

LITIGATION REVIEW ☒	r.g.f. (examiner initials)	02/27/2012 (date)
Case Name		Director Initials
VirnetX v. Cisco et al., 610cv00417, pending.		DTR ↓ TY
VirnetX v. Mitel et al., 611cv00018, pending.		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
1. Inter Partes Reexamination	95001788

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,851	12/13/2011	7418504	43614.101	1688

22852 7590 10/10/2012

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

EXAMINER	
ART UNIT	PAPER NUMBER

DATE MAILED: 10/10/2012

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

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

David L. McCombs
HAYNES AND BOONE, LLP, IP SECTION
2323 Victory Avenue, Suite 700
Dallas, TX 75219

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NUMBER *95/001,851*.

PATENT NUMBER *7,418,504*.

TECHNOLOGY CENTER *3900*.

ART UNIT *3992*.

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

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

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

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

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
95/001,851	13 December, 2011	7418504	43614.101

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

EXAMINER	
ROLAND FOSTER	
ART UNIT	PAPER
3992	20121003

DATE MAILED:

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

Commissioner for Patents

This Office communication clarifies that, in accordance with the Form PTOL-2065 (Paper No. 20120920) attached to the Action Closing Prosecution mailed October 1, 2012 ("ACP"), the patent owner may once file a submission under 37 CR 1.951(a) within 2 months from the mailing date of said ACP. The conclusion of the ACP (page 57) incorrectly states the patent owner has one month (30 days).

The examiner also withdraws all rejections of claim 11 and confirms this claim as patentable over the applied prior art of record for the reasons stated in the ACP (e.g., pages 30, 44, 53 & 54). Form PTO-2065 incorrectly states claim 11 stands rejected.

This Office communication merely clarifies positions set forth in the ACP and thus is directed to formalities only.

/Roland G. Foster/
Primary Examiner, CRU 3992

PTO-90C (Rev.04-03)

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,851
U.S. Patent No. 7,418,504	Group Art Unit: 3992
Issued: August 26, 2008	Examiner: Roland G. Foster
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	Confirmation No.: 1688
	VIA EFS WEB

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

Dear Commissioner:

PATENT OWNER'S PETITION FOR EXTENSION OF TIME PURSUANT TO 37 C.F.R. § 1.956

VirnetX Inc., the owner of the above-referenced patent, hereby petitions for a one-month extension of time for responding to the Office Action mailed October 1, 2012 ("Office Action"), in the above-identified reexamination proceeding ("the '1,851 proceeding"). A response to the Office Action is currently due on December 1, 2012.

Pursuant to 37 C.F.R. § 1.956, this petition for an extension of time (1) is being filed well before the due date for the response, and (2) sets forth sufficient reasons for the extension, as detailed below. VirnetX is concurrently submitting payment of the requisite fee. If any additional fees are due, please charge them to Deposit Account 06-0916.

VirnetX's counsel has begun preparing a response to the Office Action. VirnetX, however, seeks an extension of time of one month to allow VirnetX additional time to prepare and file a suitable response.

The nature and complexity of the Office Action warrant an extension of time of one month. The Office Action itself is 60 pages in length, and it contains 21 grounds of rejection based on 18 different references. In doing so, the Office Action addresses positions in the Request for Reexamination filed December 13, 2011 and other filings in this proceeding. Accordingly, analyzing the Office Action and preparing a complete response will require substantial time and effort.

Additionally, a complete response to the Office Action may require an accompanying declaration from VirnetX's expert. VirnetX is working with its expert and investigating the need for such a declaration. Coordinating with the expert and preparing a declaration may take additional time.

Finally, VirnetX is concurrently involved in several other pending reexamination proceedings—namely, control nos. 95/001,679 and 95/001,682 involving U.S. Patent No. 6,502,135, control nos. 95/001,697 and 95/001,714 involving U.S. Patent No. 7,490,151, control no. 95/001,746 involving U.S. Patent No. 6,839,759, control no. 95/001,788 involving the '504 patent, control nos. 95/001,789 and 95/001,856 involving U.S. Patent No. 7,921,211, control no. 95/001,792 involving U.S. Patent No. 7,188,180, and control no. 95/001,949 involving U.S. Patent No. 8,051,181. These proceedings will demand attention from VirnetX and strain its resources during the period for response to the Office Action. For example, the Office recently issued office actions in the '1,788, '1,789, '1,792, and '1,856 proceedings. These office actions currently have deadlines for response within the same timeframe as the deadline for responding to the instant Office Action, meaning that VirnetX must work to prepare all of these responses in parallel. Tending to these other proceedings while preparing a response to the instant Office Action will require, by any standard, a very

significant amount of time and effort. Declarations also may be used in these proceedings, meaning that VirnetX will be coordinating with its expert to concurrently prepare multiple responses and declarations.

In view of the foregoing, VirnetX requests an extension of time of one month to complete the response to the Office Action currently due on December 1, 2012.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 7, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,851
U.S. Patent No. 7,418,504	Group Art Unit: 3992
Issued: August 26, 2008	Examiner: Roland Foster
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	Confirmation No.: 1688

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

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Petition for Extension of Time Pursuant to 37 C.F.R. § 1.956 was served by first-class mail on November 7, 2012, on counsel for the third party requester at the following address:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219-7672

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 7, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Patent Application Fee Transmittal

Application Number:	95001851
Filing Date:	13-Dec-2011
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Filer:	Joseph Edwin Palys./connie sisk
Attorney Docket Number:	43614.101

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**200**

Electronic Acknowledgement Receipt

EFS ID:	14166798
Application Number:	95001851
International Application Number:	
Confirmation Number:	1688
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Customer Number:	22852
Filer:	Joseph Edwin Palys./connie sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.101
Receipt Date:	07-NOV-2012
Filing Date:	13-DEC-2011
Time Stamp:	09:54:00
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$200
RAM confirmation Number	20054
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		EOT_504.pdf	137076 2b127f0622f02539dc77e54c82294b91056e58c5	yes	4

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Reexam Request for Extension of Time	1	3
Reexam Certificate of Service	4	4

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30324 44985bd97e3b686b3587ef7cba0d993d0f500b51	no	2

Warnings:

Information:

Total Files Size (in bytes):	167400

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,851	12/13/2011	7418504	43614.101	1688

22852 7590 11/08/2012

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

EXAMINER	
FOSTER, ROLAND G	
ART UNIT	**PAPER NUMBER**
3992	

MAIL DATE	DELIVERY MODE
11/08/2012	PAPER

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

DAVID L. MCCOMBS
HAYNES AND BOONE, LLP, IP SECTION
2323 VICTORY AVE., SUITE 700
DALLAS, TX 75219

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NUMBER *95/001,851*.

PATENT NUMBER *7,418,504*.

TECHNOLOGY CENTER *3999*.

ART UNIT *3992*.

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

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

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

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

Decision on Petition for Extension of Time in Reexamination	Control No.: 95/001,851

1. THIS IS A DECISION ON THE PETITION FILED 7 November 2012.

2. THIS DECISION IS ISSUED PURSUANT TO:
   A. ☐ 37 CFR 1.550(c) – The time for taking any action by a patent owner in an *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   B. ☒ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS
   Patent owner requests that the period for responding to the Office action mailed on 1 October 2012, which sets a two (2) month period for filing a response thereto, be extended by one (1) month.

   A. ☒ Petition fee per 37 CFR §1.17(g)):
      i. ☒ Petition includes authorization to debit a deposit account.
      ii. ☐ Petition includes authorization to charge a credit card account.
      iii. ☐ Other: _____.
   B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
   C. ☒ Petition was timely filed.
   D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
   A. ☒ Granted or ☐ Granted-in-part for one (1) month, because petitioner provided a factual accounting that established sufficient cause. (See 37 CFR 1.550(c) and 37 CFR 1.956).
      ☐ Other/comment: _____.
   B. ☐ Dismissed because:
      i. ☐ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).
      ii. ☐ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
      iii. ☐ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
      iv. ☐ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
      v. ☐ The petition is moot.
      vi. ☐ Other/comment: _____.

5. CONCLUSION

   Telephone inquiries with regard to this decision should be directed to Daniel Ryman at (571)272-3152. In his/her absence, calls may be directed to Sudhanshu Pathak at (571)272-5509 in the Central Reexamination Unit.

/Daniel Ryman/	Supervisory Patent Examiner
[*Signature*]	(Title)

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,851
U.S. Patent No. 7,418,504	Group Art Unit: 3992
Issued: August 26, 2008	Examiner: Roland G. Foster
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	Confirmation No.: 1688
	VIA EFS WEB

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

Dear Commissioner:

PATENT OWNER'S PETITION TO REOPEN PROSECUTION PURSUANT TO 37 C.F.R. § 1.181

VirnetX Inc., the owner of the above-referenced patent, submits that the Action Closing Prosecution in the above-identified reexamination proceeding was premature, and hereby requests that the Director reopen prosecution.

To the extent that entry and consideration of this petition require suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. In addition, if there is any fee due in connection with the filing of this petition, please charge the fee to Deposit Account 06-0916.

I. Background

Third-party requester Cisco Systems, Inc. ("Cisco") filed a Request for Reexamination ("Request") on December 13, 2011. The Request, asserting 18 different references in support of 21

proposed grounds of rejection, is 39 pages long and additionally incorporates 328 pages of claim charts.

The Request was granted and the Office issued a first Office Action ("OA") on March 1, 2012, which adopted each of Cisco's 21 proposed rejections. In support of the rejections, the OA incorporated by reference 18 pages of the Request plus the Request's 328 pages of claim charts, for a total of 346 pages.

VirnetX filed a response ("Response") to the Office Action on June 1, 2012.

Cisco filed third-party comments ("Comments") to VirnetX's Response on June 29, 2012.

The Office issued an Action Closing Prosecution ("ACP") on October 1, 2012, withdrawing 5 of the 21 rejections proposed in the Request, and maintaining or modifying the remaining 16 proposed rejections, again incorporating by reference the combined 346 pages of the Request and its claim charts. In addition, the ACP provides new bases for its rejections, adopts new claim constructions, and responds to only a subset of arguments made in VirnetX's Response.

II. Argument

VirnetX respectfully submits that the ACP was premature. The M.P.E.P. instructs that an ACP is improper if the issues have not been fully developed. M.P.E.P. § 2671.01 (citing 37 C.F.R. 1.949). The M.P.E.P. also states that "an ACP must . . . include a rebuttal of any arguments raised in the patent owner's response . . . ." (*Id.* at § 2671.02.) Here, the ACP rejects claims on new grounds introduced for the first time in the ACP. The ACP also does not consider or respond to several arguments raised in VirnetX's Response. Thus, the Office has maintained rejections based on new arguments for which VirnetX had no opportunity to respond, or simply sided with many of Requestor's positions without articulating a reasonable explanation for having done so. As a result, the parties have not been given a sufficient opportunity to develop the issues in this proceeding. Prosecution should therefore be reopened.

First, the ACP is premature because the Office introduces claim constructions for the first time in the ACP. (*Id.* at 19-22, "Claim Interpretation.") The Office adopts constructions of important claim features, such as "domain name service system" and "indication," neither of which were included in the first Office Action. (*Id.*) These claim constructions are also inconsistently applied throughout the ACP to maintain the rejections, or not applied at all. For example, the ACP construes the "indication" recited in claim 1 as "a visible message or signal to a user." (*Id.*) But it then rejects the claims over references allegedly disclosing, among other things, the returning of network addresses or key records, all without explaining how such actions constitute "a visible message or signal to a user," and without considering whether they are in fact hidden from a user or transparent to a user. (*See, e.g.*, *id.* at 31-36, 45-48.) VirnetX has not had any opportunity to address these claim constructions or the manner in which they have been applied. Thus, the ACP was premature because these issues require further development.

Second, the ACP adds new grounds of rejection. For example, the Office asserts for the first time in the ACP that claims 24 and 48 are directed to nonfunctional descriptive matter. (*Id.*; *compare* OA at 11, incorporating Req. Ex. F-1 at 37-38.) This basis for the rejection was not raised in the first Office Action or the Request, and therefore VirnetX has had no opportunity to respond. As a result, the ACP was premature and prosecution should be reopened so that the parties may have an opportunity to address these new grounds presented in the ACP.

Third, the ACP does not fully address many of the arguments VirnetX asserted in its Response. For instance, VirnetX traversed the rejection of claims 24 and 48 based on *Lendenmann* as not supported by the teachings of *Lendenmann*. (Response at 18-19.) But in the ACP, the Office simply repeated its prior basis for the rejection without addressing VirnetX's traversal, stating that that VirnetX's arguments were "unpersuasive[]" without addressing their substance. (ACP at 27-28.) Because VirnetX's arguments remain unaddressed, while the Office adds new grounds of rejection,

many important issues have not been fully developed. Accordingly, the ACP was premature and prosecution should be reopened.

As another example, VirnetX traversed the rejection of claim 27 based on *Kiuchi* in view of *Pfaffenberger* because the combination does not disclose or suggest a "domain name service system . . . configured to enable establishment of a secure communication link . . . ." (Response at 65.) The Office maintained the rejection of claim 27, but only addressed the rejection of claim 26. (ACP at 53.) By failing to address VirnetX's arguments here as well, many important issues have not been fully developed and prosecution should be reopened. M.P.E.P. § 2671.02 ("an ACP must . . . include a rebuttal of any arguments raised in the patent owner's response . . . .").

The M.P.E.P. instructs that the Office should be liberal in reopening prosecution where the equities of the situation render such action appropriate, because a patent owner cannot continue the proceeding by re-filing under 37 C.F.R. 1.53(b) or 1.53(d), or by filing a Request for Continued Examination under 37 C.F.R. 1.114. *See* M.P.E.P. 2673.01. Additionally, 37 C.F.R. § 1.183 provides that "in an extraordinary situation, *when justice requires*, any requirement of the regulation in this part which is not a requirement of the statutes may be suspended or waived by the director or the director's designee . . . on petition of the interested party." (Emphasis added.)

Here, justice requires reopening prosecution. The Office was required to navigate the Request for Reexamination and its claim charts—a combined 367 pages—presenting 21 grounds of rejection under 35 U.S.C. §§ 102 and 103 based on 18 references, either alone or in combination. It appears that Requester Cisco has successfully utilized the sheer volume of the Request and other papers in this proceeding to prevent a full development of the issues, as many grounds for the rejections have just recently been clarified or asserted for the first time in the ACP. But since the ACP removes VirnetX's opportunity to fully address the new issues raised in the ACP and reassert its prior unaddressed arguments, VirnetX's ability to respond to Cisco's incorrect allegations has

been severely compromised. Accordingly, the ACP was premature and prosecution should be reopened to fully develop the issues in this proceeding.

III. Conclusion

In view of the foregoing, VirnetX submits that the premature timing of the ACP compromises VirnetX's opportunity to fully address the issues raised in this proceeding, and respectfully requests that the Director reopen prosecution.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 3, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket No. 11798.0007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	
Victor Larson et al.	Control No.: 95/001,851
U.S. Patent No. 7,418,504	Group Art Unit: 3992
Issued: August 26, 2008	Examiner: Roland G. Foster
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	Confirmation No.: 1688

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

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Petition to Reopen Prosecution Pursuant to 37 C.F.R. § 1.181 was served by first-class mail on December 3, 2012, on counsel for the third party requester at the following address:

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 3, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14362766
Application Number:	95001851
International Application Number:	
Confirmation Number:	1688
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Customer Number:	22852
Filer:	Joseph Edwin Palys./Connie Sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.101
Receipt Date:	03-DEC-2012
Filing Date:	13-DEC-2011
Time Stamp:	09:47:38
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Petition_To_Reopen_851.pdf	233542 80e7b048d255e832d0ce2da94a528d5e326f5165	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Receipt of Petition in a Reexam	1	5
	Reexam Certificate of Service	6	6
Warnings:			
Information:			
	Total Files Size (in bytes):	233542	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket Nos. 11798.0007; 11798.0011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor LARSON et al.	)	Control Nos.: 95/001,851; 95/001,788
	)	
U. S. Patent No. 7,418,504	)	Group Art Unit: 3992
	)	
Issued: August 26, 2008	)	Examiner: Roland G. Foster
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	)	Confirmation Nos. 1688; 5823

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

Dear Commissioner:

REVOCATION OF POWER OF ATTORNEY,
STATEMENT UNDER 37 C.F.R. § 3.73(b),
AND GRANT OF NEW POWER OF ATTORNEY

The undersigned, a representative authorized to sign on behalf of the assignee owning all of the interest in U.S. Patent No. 7,418,504 ("the '504 patent"), hereby revokes all previous powers of attorney or authorization of agent granted in the '504 patent before the date of execution hereof.

In compliance with 37 C.F.R. § 3.73(b), the undersigned verifies that VirnetX Inc. is the assignee of the entire right, title, and interest in the '504 patent by virtue of an assignment recorded in the U.S. Patent and Trademark Office at Reel 018757, Frame 0326 on January 10, 2007.

The undersigned representative of the assignee hereby grants its power of attorney to the patent practitioners associated with **Finnegan, Henderson, Farabow, Garrett & Dunner,**

L.L.P., Customer Number 22,852, to transact all business in the Patent and Trademark Office connected with the '504 patent, including the reexamination proceedings assigned control nos. 95/001,851 and 95/001,788, and in any other proceedings involving the '504 patent.

Please also send all future correspondence concerning the '504 patent to the address associated with **Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., Customer Number 22,852.**

Dated: 11/30/12

By: _____

Sameer Mathur
Vice President, Corporate Development and Product Marketing
VirnetX Inc.

PATENT
Customer No. 22,852
Attorney Docket Nos. 11798.0007; 11798.0011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor LARSON et al.	)	Control Nos.: 95/001,851; 95/001,788
	)	
U. S. Patent No. 7,418,504	)	Group Art Unit: 3992
	)	
Issued: August 26, 2008	)	Examiner: Roland Foster
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	)	Confirmation Nos. 1688; 5823

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

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and M.P.E.P. § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Revocation of Power of Attorney, Statement Under 37 C.F.R. §3.73(b), and Grant of New Power of Attorney was served by first-class mail on December 3, 2012, on counsel for the third party requesters at the following addresses:

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: December 3, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14367620
Application Number:	95001851
International Application Number:	
Confirmation Number:	1688
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Customer Number:	22852
Filer:	Joseph Edwin Palys./connie sisk
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.101
Receipt Date:	03-DEC-2012
Filing Date:	13-DEC-2011
Time Stamp:	15:19:10
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Reexam_POA_851_and_788.pdf	88544 7d4862cade57b4f11b13dc802980c65e8efa2ac4	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Reexam Change in Pwr Atty for Third Party Requester	1	2
	Reexam Certificate of Service	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	88544	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,851	12/13/2011	7418504	43614.101

CONFIRMATION NO. 1688

POA ACCEPTANCE LETTER

22852
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

OC000000057963880

Date Mailed: 12/04/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/03/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/pavolpe/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,851	12/13/2011	7418504	43614.101

CONFIRMATION NO. 1688

POWER OF ATTORNEY NOTICE

22852
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

OC000000057963897

Date Mailed: 12/04/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/03/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/pavolpe/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the PETITION UNDER 37 CFR § 1.182 TO SHORTEN RESPONSE PERIODS AND ACCELERATE PROCEEDINGS was served on:

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

the attorneys of record for the assignee of USP7921211 and of record for the assignee in the '1679, '1851, '1856, '1746, and '1792 reexamination proceedings, and on:

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington DC 20001

the attorneys of record for the assignee of USP 6502135, USP 7490151, USP 7418504, USP 6839759, and USP 7188180 and of record for the assignee in the '1714 reexamination proceeding, and on:

Sidley Austin LLP
1501 K Street N.W.
Washington, DC 20005

the attorneys of record for Apple Inc. in the merged '1714 and '1697 reexamination proceedings, all done in accordance with 37 CFR § 1.903, on December 5, 2012.

/David L. McCombs/

David L. McCombs,
Registration No. 32,271

Electronic Patent Application Fee Transmittal

Application Number:	95001851
Filing Date:	13-Dec-2011
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Filer:	David L. McCombs/Theresa O'Connor
Attorney Docket Number:	43614.101

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION IN REEXAM PROCEEDING	1824	1	1930	1930
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**1930**

Electronic Acknowledgement Receipt

EFS ID:	14389338
Application Number:	95001851
International Application Number:	
Confirmation Number:	1688
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Customer Number:	22852
Filer:	David L. McCombs/Theresa O'Connor
Filer Authorized By:	David L. McCombs
Attorney Docket Number:	43614.101
Receipt Date:	05-DEC-2012
Filing Date:	13-DEC-2011
Time Stamp:	14:24:28
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1930
RAM confirmation Number	851
Deposit Account	081394
Authorized User	MCCOMBS, DAVID L

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Petition_to_Shorten.pdf	200572 28ab80f8745412b95b3969e459904e3f2cab1ba4	yes	5

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Receipt of Petition in a Reexam	1	4
Reexam Certificate of Service	5	5

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30341 88c67938ae444a16c3f83b0bdba5814e1e65f5f2	no	2

Warnings:

Information:

Total Files Size (in bytes):	230913

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Customer No. 22,852
Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 6,502,135 Edmund Munger et al.	Control Nos.: 95/001,679 95/001,682 Examiner: Behzad Peikari
In re U.S. Patent No. 7,490,151 Edmund Munger et al.	Control Nos.: 95/001,714 95/001,697 Examiner: Michael J. Yigdall
In re U.S. Patent No. 6,839,759 Victor Larson et al.	Control No. 95/001,746 Examiner: Salman Ahmed
In re U.S. Patent No. 7,188,180 Victor Larson et al.	Control No.: 95/001,792 Examiner: Deandra M. Hughes
In re U.S. Patent No. 7,418,504 Victor Larson et al.	Control No.: 95/001,851 Examiner: Roland G. Foster
In re U.S. Patent No. 7,921,211 Victor Larson et al.	Control No.: 95/001,856 Examiner: Roland G. Foster

VIA EFS WEB

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

Dear Commissioner:

PATENT OWNER'S PETITION IN OPPOSITION TO THIRD-PARTY REQUESTER CISCO SYSTEMS, INC.'S PETITION TO SHORTEN RESPONSE PERIODS AND ACCELERATE PROCEEDINGS

VirnetX Inc., the owner of the above-referenced patents, opposes third-party requester Cisco Systems, Inc.'s Petition Under 37 CFR § 1.182 to Shorten Response Periods and Accelerate Proceedings ("Petition"). Cisco's dissatisfaction with the progress of the reexaminations is the direct

result of Cisco's own delays and strategic decisions during these proceedings. As a result, the relief sought in the Petition should not be granted, especially since it prejudices the patent owner VirnetX.

If entry and consideration of this petition requires suspension of any rules, suspension is requested pursuant to 37 C.F.R. § 1.183. And if any fee is due in connection with the filing of this petition, please charge it to Deposit Account 06-0916.

I. Background

A. Control Nos. 95/001,679 and 95/001,682

Cisco filed its Request for Reexamination of U.S. Patent No. 6,502,135 ("the '135 patent") on July 8, 2011. The Office granted the Request and ordered reexamination on October 3, 2011. The Office issued an Office Action on February 15, 2012. Patent Owner timely filed a Response to the Office Action on May 15, 2012, and Cisco filed Comments on June 14, 2012. The Office merged this proceeding on December 13, 2012 with a separate reexamination involving the '135 patent. That other reexamination bears control no. 95/001,682 and names Apple Inc. ("Apple") as the real party in interest.

B. Control Nos. 95/001,714 and 95/001,697 ("the '1,697 proceeding")

Cisco filed its Request for Reexamination of U.S. Patent No. 7,490,151 ("the '151 patent") on August 16, 2011. The Office granted the Request and ordered reexamination on October 31, 2011. The Office merged this proceeding on March 15, 2012 with a separate reexamination involving the '151 patent. That other reexamination bears control no. 95/001,697 and names Apple as the real party in interest. The Office issued an Office Action in the merged proceedings on April 20, 2012. Patent Owner timely filed a Response to the Office Action on July 20, 2012, and Cisco filed Comments on August 17, 2012.

C. Control No. 95/001,746 ("the '746 proceeding")

Cisco filed its Request for Reexamination of U.S. Patent No. 7,839,759 ("the '759 patent") on September 7, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on October 14, 2011. Patent Owner timely filed a response to the Office Action on January 17, 2012, and Cisco filed Comments on February 15, 2012.

The Office issued a second Office Action on June 18, 2012. Patent Owner timely filed a response to the second Office Action on August 20, 2012, and Cisco filed Comments on September 18, 2012.

D. Control No. 95/001,792 ("the '792 proceeding")

Cisco filed its Request for Reexamination of U.S. Patent No. 7,188,180 ("the '180 patent") on October 25, 2011. The Office denied the Request on December 17, 2011. Cisco filed a petition challenging the Office's denial of the Request on January 17, 2012. The Office granted-in-part Cisco's petition on September 6, 2012, ordered reexamination, and issued an Office Action on September 19, 2011, which remains pending.

E. Control No. 95/001,851 ("the '1,851 proceeding")

Cisco filed its Request for Reexamination of U.S. Patent No. 7,418,504 ("the '504 patent") on December 13, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on March 1, 2012. Patent Owner timely filed a response to the Office Action on June 1, 2012, and Cisco filed Comments on June 29, 2012. The Office issued a second Office Action on October 1, 2012, which remains pending.

F. Control No. 95/001,856 ("the '1,856 proceeding")

Cisco filed its Request for Reexamination of U.S. Patent No. 7,921, 211 ("the '211 patent") on December 16, 2011. The Office granted the Request, ordered reexamination, and issued an Office Action on March 5, 2012. Patent Owner timely filed a response to the Office Action on June 5,

2012, and Cisco filed Comments on July 3, 2012. The Office issued a second Office Action on October 1, 2012, which remains pending.

G. Litigation in the Eastern District of Texas

Patent Owner asserted the '135, '759, '180, and '504 patents in a Complaint filed against Cisco on August 11, 2010 in the Eastern District of Texas (*VirnetX Inc. v. Cisco Sys., Inc., et al.*, No. 6:10-cv-00417). Patent Owner additionally asserted the '151 and '211 patents in an Amended Complaint filed against Cisco on April 5, 2011. Cisco and its co-defendant, Apple, filed a sealed motion for separate trials on August 31, 2012. The court granted the motion, set Apple's trial date for October 31, 2012, and set Cisco's trial date for March 11, 2013.

Apple and Patent Owner recently concluded their trial. On November 6, 2012, the jury found the asserted claims of the '135, '151, '504, and '211 patents valid and infringed by Apple, awarding Patent Owner over $368 million in damages. (Ex. A-10.)

II. Argument

As its trial date approaches, Cisco asserts that the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, 95/001,856 proceedings must be accelerated. (Petition 3.) The primary reasons the reexaminations lag so far behind the district-court action, however, are Cisco's own delays and strategic decisions during these proceedings. The Office should not grant the extraordinary relief sought by Cisco for at least these reasons and for the other reasons discussed below.

First, Cisco did not begin to file these reexamination requests until eleven months after the litigation began, and delayed in some instances for up to sixteen months. Cisco has been on notice of Patent Owner's infringement claims based on the '135, '759, '180 and '504 patents at least since Patent Owner filed its first Complaint on August 11, 2010. Yet Cisco did not file requests for reexamination of the '135, '759, '180 and '504 patents until July 8, 2011, September 7, 2011,

October 25, 2011, and December 13, 2011, respectively. Due to Cisco's delays of up to sixteen months in filing, the prosecution of these reexaminations is still before the Central Reexamination Unit. Cisco has no basis to now request additional burdensome action on the part of the Office and the Patent Owner, having caused the very delays it seeks to remedy.

Second, these reexaminations are already being appropriately conducted by the Office with the "special dispatch" sought by Cisco. In the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings, Cisco filed enormous requests for reexamination totaling 223, 203, 231, 193, 366, and 366 pages, respectively, including appended claim charts. These requests presented proposed rejections implicating at least 44 different references—several of them well over one hundred pages long. The Office had to review and process all of these papers before issuing Office Actions, and did so within an expeditious timeframe. Cisco could have honed its invalidity positions and filed more targeted reexamination requests to streamline these proceedings, but it did not. Cisco elected to proceed with an omnibus approach to these reexaminations, and should not now be heard to complain about the Office's and Patent Owner's efforts in reviewing Cisco's vast filings and advancing these reexaminations.

Third, Cisco appears to have been content with the current schedule of the reexaminations throughout their prosecution. Having waited over a year to file many of these reexaminations, Cisco also delayed well beyond the one-year anniversaries of several of these reexamination proceedings before raising any questions regarding the speed of their schedules. (*See id.* at 3.) Cisco's newfound concern, precipitated by its co-defendant Apple's adverse jury verdict and its own now-inconvenient procrastination, does not justify accelerating these proceedings. Doing so would only further burden the Patent Owner and the Office when the Office is already responding with "special dispatch" to the enormous number of issues raised in Cisco's lengthy and late-filed reexamination requests.

Fourth, accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would also substantially prejudice Patent Owner. Along with these proceedings, Patent Owner is concurrently involved in five additional reexaminations naming Apple as the real party in interest, which are also demanding significant attention from Patent Owner. (*See* control nos. 95/001,682; 95/001,788; 95/001,789; and 95/001,949 and the merged proceedings in control nos. 95/001,697 and 95/001,714.) Accelerating the 95/001,679, 95/001,714, 95/001,746, 95/001,792, 95/001,851, and 95/001,856 proceedings would therefore unreasonably burden Patent Owner and its counsel. Patent Owner would not have sufficient time and opportunity to respond adequately within shortened time periods, given that it must also respond to filings from Apple in a large number of other reexaminations. Indeed, Patent Owner is currently preparing responses to *five* pending Office Actions. (*See* control nos. 95/001,788; 95/001,789; 95/001,792; 95/001,851; and 95/001,856).

Finally, shortening Patent Owner's response periods would not achieve any benefit in these proceedings. Cisco vaguely asserts that "[q]uickly reaching a final decision on the invalidity of the patents in reexamination . . . will ensure that the outcomes of the Office proceedings will be considered in conjunction with related proceedings." (Petition 2.) But if Cisco is referring to the litigation as the "related proceedings," the district court in fact will enter a final judgment and the litigation will reach the Federal Circuit long before the reexaminations will, given the upcoming trial date of March 11, 2013. Thus, even if the Office were to grant Cisco's request (which it should not), the reexaminations will not be ready for appeal to the Federal Circuit for quite some time. Because the relief requested will not help to align the litigation and the reexaminations, and because Cisco is seeking relief from the consequences of its own strategic decisions, shortening Patent Owner's response periods to respond to the enormous number of issues raised in Cisco's lengthy reexamination requests would be unreasonable and prejudicial.

III. Conclusion

The reexaminations are proceeding with the appropriate "special dispatch." Cisco's complaints arise chiefly from its own delay in waiting to file its requests for reexamination, as well as from its own strategic decisions during the course of these reexaminations. Moreover, the relief requested would not promote efficiency, but rather would only prejudice the Patent Owner. Indeed, hurried prosecution of these proceedings would likely result in incomplete consideration of the issues and in fact act to slow the reexaminations. In view of all of the foregoing circumstances, Patent Owner respectfully submits that Cisco's petition should be denied.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 19, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

PATENT
Customer No. 22,852
Attorney Docket Nos. 11798.0001, 0002, 0003, 0005, 0007, 0008, 0009, 0010

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent No. 6,502,135 Edmund Munger et al.	Control No.: 95/001,679 95/001,682 Examiner: Behzad Peikari
In re U.S. Patent No. 7,490,151 Edmund Munger et al.	Control Nos.: 95/001,714 95/001,697 Examiner: Michael J. Yigdall
In re U.S. Patent No. 6,839,759 Victor Larson et al.	Control No. 95/001,746 Examiner: Salman Ahmed
In re U.S. Patent No. 7,188,180 Victor Larson et al.	Control No.: 95/001,792 Examiner: Deandra M. Hughes
In re U.S. Patent No. 7,418,504 Victor Larson et al.	Control No.: 95/001,851 Examiner: Roland G. Foster
In re U.S. Patent No. 7,921,211 Victor Larson et al.	Control No.: 95/001,856 Examiner: Roland G. Foster

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

Dear Commissioner:

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 1.248 and 1.903 and MPEP § 2666.06, the undersigned attorney for the patent owner certifies that a copy of the Patent Owner's Petition in Opposition to Third-Party Requester Cisco Systems, Inc.'s Petition to Shorten Response Periods and Accelerate Proceedings was served by first-class mail on December 19, 2012, on counsel for the third party requesters at the following addresses:

Sidley Austin LLP
717 North Harwood
Suite 3400
Dallas, TX 75201

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 19, 2012

By: /Joseph E. Palys/
Joseph E. Palys
Reg. No. 46,508

Electronic Acknowledgement Receipt

EFS ID:	14514206
Application Number:	95001851
International Application Number:	
Confirmation Number:	1688
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	7418504
Customer Number:	22852
Filer:	Joseph Edwin Palys./Sheryl Lewis
Filer Authorized By:	Joseph Edwin Palys.
Attorney Docket Number:	43614.101
Receipt Date:	19-DEC-2012
Filing Date:	13-DEC-2011
Time Stamp:	15:10:52
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		OpptoCiscospetitiontoaccelerate.pdf	437556 7423eb3158846a3696be50d8eaeb55404085f9a4	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Receipt of Petition in a Reexam	1	7
	Reexam Certificate of Service	8	9
Warnings:			
Information:			
	Total Files Size (in bytes):	437556	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	Control No.: 95/001,851
Victor Larson et al.	)	
	)	Group Art Unit: 3992
U.S. Patent No. 7,418,504	)	
	)	Examiner: Roland G. Foster
Issued: August 26, 2008	)	
	)	Confirmation No.: 1688
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	)	

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

Dear Commissioner:

PATENT OWNER'S RESPONSE TO OFFICE ACTION OF OCTOBER 1, 2012

On March 1, 2012, the U.S. Patent and Trademark Office ("Office") issued a first Office Action ("First OA" or "First Office Action") in these reexamination proceedings. VirnetX Inc. ("VirnetX" or "Patent Owner"), the owner of U.S. Patent No. 7,418,504 ("the '504 patent"), filed a Response ("Response") on June 1, 2012. Requester Cisco Inc. ("Cisco" or "Requester") filed Comments ("Comments") on June 29, 2012. On October 1, 2012, the Office issued a second Office Action ("Second OA" or "Second Office Action"), which was an Action Closing Prosecution ("ACP"), in these proceedings.

Claims 1-60 are patentable at least for the reasons that follow and the reasons stated in VirnetX's June 1, 2012, Response. Thus, VirnetX requests that claims 1-60 be confirmed. This Response is supported by a Supplemental Declaration of Angelos D. Keromytis, Ph.D. ("Supp. Keromytis Decl."). At times, this Response also refers to the initial Declaration of Angelos D. Keromytis, Ph.D. ("Keromytis Decl.") supporting the Response filed on June 1, 2012.

I. Confirmed Claim 11 and Withdrawn Rejections (Issues 2, 6, 10, 14, and 19)

Patent Owner appreciates the Office's recognition in a supplemental communication mailed October 10, 2012, that all of the previous rejections of claim 11 have been withdrawn and that the claim has been confirmed. Patent Owner also appreciates that the rejections identified in Issues 2, 6,

10, 14, and 19 have been withdrawn in their entirety. (Second OA at 4.) Patent Owner asserts that those rejections should remain withdrawn for at least the reasons discussed in the Response.

The Office maintains the rejections, in whole or in part, identified in Issues 1, 3-5, 7-9, 11-13, 15-18, 20, and 21. For the reasons discussed below, these rejections should also be withdrawn and all claims 1-60 should be confirmed.

II. The Maintained Rejections Are Based on Improper Claim Constructions

The Office's rejections for Issues 1, 3-5, 7-9, 11-13, 15-18, 20, and 21 are improper because the Office takes incorrect positions on claim construction. In some instances, the Office proposes unreasonably broad constructions, stretching the '504 patent claims beyond their proper scope to read on the asserted references. In other instances, the Office advocates constructions that are inconsistent with clear disclaimers in the '504 patent specification. Still in others, the Office does not apply the claim construction it elsewhere purports to adopt. These are effectively new claim-construction positions taken in the ACP, which Patent Owner has not had a chance to rebut. Given these new positions advocated by the Office, the latest Office Action should not have been an ACP.[1] *See* M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed."). Moreover, as explained below, even under the new positions raised in the ACP, the Office has not demonstrated that the claims are unpatentable.

A. Standards for Claim Construction

"During reexamination, claims are given the broadest reasonable interpretation consistent with the specification . . . ." M.P.E.P. § 2258(I)(G); *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1148 (Fed. Cir. 2012). But while "the USPTO must give claims their broadest reasonable interpretation in light of the Specification," this does not mean that it may construe a claim term to have an atypical meaning. *In re Kuibira*, Appeal No. 2009-002409, 2010 WL 390100, at *2 (B.P.A.I. Feb. 1, 2010). Instead, "the words of the claim must be given their *ordinary* meaning unless the ordinary meaning is inconsistent with the Specification." *Id.* (emphasis added). As the Board noted, "the purpose [of giving claims their broadest reasonable interpretation] is not to stretch the interpretation of a claim limitation beyond what would be reasonably understood by the skilled worker in the light of the Specification, to read on a prior art structure which could possibly, but not

[1] The Second Office Action should not have been an ACP, so Patent Owner requests a new, nonfinal Office Action for at least the reasons discussed in Patent Owner's Petition to Reopen Prosecution Pursuant to 37 C.F.R. § 1.181, filed December 3, 2012. Patent Owner notes that Requester has asserted, incorrectly, that the December 3, 2012, Petition included a substantive response on the merits of the Second Office Action. (*See* Requester's Submission of December 19, 2012.) This is, of course, incorrect. The December 3, 2012, Petition, clearly titled a "Petition to Reopen Prosecution," was directed solely to topics supporting the Petition and did not include any substantive response on the merits.

reasonably, be covered by it." *In re Alferness*, Appeal No. 2009-0122, 2009 WL 1171349, at *6 (B.P.A.I. Apr. 30, 2009). Given the Federal Circuit's and the Board's focus on reading claims in light of the specification, the Examiner is not free to disregard plain statements in the specification disclaiming certain embodiments from the scope of the claimed invention.

B. The Rejections Are Based on Incorrect Constructions of the Claimed "Domain Name Service System"

Independent claim 1 recites "a *domain name service system* configured to . . . comprise an indication that the *domain name service system* supports establishing a secure communication link" (emphases added). Independent claims 36 and 60 also recite a "domain name service system." Accordingly, every claim of the '504 patent expressly recites, or incorporates by virtue of its dependency, features relating to a "domain name service system" ("DNS system"). (*See* '504 patent 55:49-60:14.) The Office's construction of the claimed "DNS system," however, is unreasonably broad.

In construing "DNS system," the Office states that a DNS system can include a single "DNS device" or multiple "DNS devices." (Second OA at 19-22, referring to sections of the '504 patent that discuss the roles of gatekeeper 2603, DNS proxy 2610, and DNS server 2609.) The Office then stretches this understanding to contend that virtually any device—regardless of whether it has any DNS functionality—may be a "DNS device" as long as it is in the same network as at least one device that actually has DNS functionality. Indeed, the Office construes a "DNS system" and interprets a "DNS device" as having no bounds whatsoever, and it applies those terms accordingly. (*See id.*)

Through these constructions, the Office has stretched the recited DNS system beyond its proper scope to encompass, in the asserted references, devices that one of ordinary skill in the art would have viewed as *non*-DNS devices, *outside* the scope of a DNS system. (Supp. Keromytis Decl. ¶¶ 8-9.) For example, the Office contends that *Aziz*'s authorized client 210, which *sends a DNS request* to a name server, is part of the claimed DNS system. (*See infra* Section IV.) If the Office's unbounded view of a DNS device is correct, virtually *any* component, if connected to a computing network that has DNS functionality somewhere within it (e.g., the Internet), qualifies as a DNS device within a DNS system. The Office's construction is simply unreasonably broad and is inconsistent with how one of ordinary skill in the art would have understood a DNS system, particularly in light of the '504 patent specification.

The Office relies on the '504 patent's description of gatekeeper 2603, DNS proxy 2610, and DNS server 2609 to support its unreasonable interpretation of a DNS system. However, the

'504 patent discloses significant DNS functionality and coordination between these devices in acting upon a DNS request. For example, the '504 patent specification explains that, in one scenario, DNS proxy 2610 receives a DNS request, determines that the DNS request is for a nonsecure target site, and passes the DNS request through to DNS server 2609 for resolution to the client. ('504 patent 40:6-8, 40:25-29, 40:53-56.) Thus, DNS proxy 2610 and DNS server 2609 interact with each other to process a DNS request, and the client need not run separate lookups with both the proxy and the server. (*Id.*) Alternatively, DNS proxy 2610 may determine that the DNS request is for a secure target site, perform an authorization check, transmit a message to gatekeeper 2603 to facilitate creating a VPN link, and obtain a resolved address from the gatekeeper 2603 to return to the client. (*Id.* at 40:6-24, 40:57-59.) Again, in this scenario, the DNS proxy 2610 and the gatekeeper 2603 interact together to process a DNS request, and the client need not run separate lookups with the proxy and the gatekeeper. (*Id.*) These devices all have significant DNS functionality, and any assertion that DNS devices may include devices not having actual DNS functionality directly contradicts the explicit and consistent teachings of the '504 patent specification. By doing just this, the Office adopts an unreasonable construction of a DNS system with no outer limits that sweeps in non-DNS devices. (Supp. Keromytis Decl. ¶¶ 7-9.) The '504 patent specification does not support the Office's unbounded interpretation.

For these reasons and those discussed in greater detail below, the rejections are based on an improper construction of the claimed DNS system and should be withdrawn.

C. The Rejections Are Based on Incorrect Constructions of the Claimed "Indication"

Every claim of the '504 patent also recites, or incorporates by virtue of its dependency, the feature of "an indication that the domain name service system supports establishing a secure communication link." (*See* '504 patent 55:49-60:14.) The Office's construction of the recited "indication" is also incorrect and renders the Office's patentability conclusions defective for at least two reasons. First, the Office adopts a construction of the claimed indication but then concludes that the cited references disclose this feature without ever applying its construction. Second, the Office instead implicitly adopts a second, unreasonably broad construction that is disclaimed in the '504 patent specification. Thus, as discussed in greater detail below, the Office's rejections should be withdrawn.

The Office construes the recited "indication" term as "a visible message or signal to a user that the DNS system supports establishing a secure communication link." (Second OA at 21-22, citing Apple Comments, Ex. A, in control no. 95/001,788.) But the Office never applies this

construction when attempting to show how the references allegedly disclose the recited indication. As one example, the Office asserts that *Aziz*'s returning of IP addresses, public keys, and authentication signatures discloses the recited indication, without explaining how doing so provides a "visible message or signal to a user." (*See, e.g.*, *id.* at 31-37.) In fact, those skilled in the art would have understood that returning IP addresses, keys, and digital signatures would not have been *visible* messages or signals *to a user*. (Supp. Keromytis Decl. ¶ 11.) The Office similarly omits this analysis in rejections based on other references.

Although VirnetX does not agree with the Office's purported claim construction, VirnetX's ability to challenge the application of its construction is significantly hampered because the Office has not explained how it should be applied. As a result, Patent Owner has to guess as to the true basis for the rejection, improperly placing the burden of establishing a prima facie case of anticipation on Patent Owner rather than the Office. *In re Jung*, 637 F.3d 1356, 1362 (Fed. Cir. 2011) ("The Patent and Trademark Office ('PTO') satisfies its initial burden of production by 'adequately explain[ing] the shortcomings it perceives so that the applicant is properly notified and able to respond.'" (alteration in original) (citation omitted)). By concealing the basis for its rejection in this manner, the Office has also contravened 35 U.S.C. § 132. *Chester v. Miller*, 906 F.2d 1574, 1578 (Fed. Cir. 1990) (Section 132 is violated "when a rejection is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection").

The Second Office Action also applies a much broader construction of "indication" that encompasses features that neither indicate that the domain name service system supports establishing a secure communication link nor are visible to any users, such as merely returning an IP address, public key, or digital authentication signature. (*See, e.g.*, Second OA at 31, stating that "returning a network address corresponding to a . . . firewall" teaches an indication within the meaning of the claims; *id.* at 35, "returning public keys and digital signatures corresponding to a secure domain name teaches [the recited indication].") The Office's construction is improper because it is inconsistent with the '504 patent specification. M.P.E.P. § 2258(I)(G) ("During reexamination, claims are given the broadest reasonable interpretation *consistent with the specification* . . . ." (emphasis added)); *see also Abbott*, 696 F.3d at 1149 ("Usually [the specification] is dispositive; it is the single best guide to the meaning of a disputed term." (citation omitted)).

The '504 patent specification clearly and unequivocally disclaims merely returning an address or a public key by describing these actions as "conventional" in the prior art:

> *Conventional* Domain Name Servers (DNSs) provide a look-up function that *returns the IP address* of a requested computer or host. . . .

> One *conventional* scheme that provides secure virtual private networks over the Internet *provides the DNS server with public keys* of the machines that the DNS server has the address for. This *allows hosts to retrieve automatically the public keys* of a host that the host is to communicate with . . . . One implementation of this standard is presently being developed as part of the Free S/WAN project (RFC 2535).

('504 patent 39:7-42, emphases added.) The specification explains that DNS systems that perform no more than these conventional functions have many shortcomings, and further explains novel DNS-system embodiments that go beyond these conventional functions by supporting establishing secure communications. (Supp. Keromytis Decl. ¶ 12.)

Furthermore, the '504 patent specification repeatedly and explicitly disparages systems with functionalities limited to the conventional IP-address and public-key features discussed above. *Abbott*, 696 F.3d at 1149-50 (holding that disparagement of features in the specification supports disclaimer). For example, the '504 patent specification explains:

> In the *conventional* architecture . . . , nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets . . . . This would hamper anonymous communications on the Internet . . . .
>
> The *conventional* scheme suffers from certain drawbacks . . . .
>
> According to certain aspects of the invention . . . , the server does not return true IP address of the target node, *but instead* automatically sets up a virtual private network . . . .
>
> Had the user requested lookup of a non-secure web site, such as site 2611, DNS proxy would *merely pass through to conventional DNS server* 2609 the look-up request, which would be handled in *a conventional manner*, returning the IP address . . . .

('504 patent 39:7-40:29, emphases added.)

Never does the specification equate the mere return of requested DNS records, such as an IP address or public key, with supporting secure communications. Indeed, in one embodiment, the DNS system does not return an IP address, "but instead automatically sets up a virtual private network between the target node and the user." (*Id.* at 39:50-51.) In another embodiment, "DNS proxy 2610 *transmits a message* to gatekeeper 2603 *requesting that a virtual private network be created* between user computer 2601 and secure target site 2604," with an IP address only being returned after the secure communication link is set up. (*Id.* at 40:12-24, emphases added.) In yet another embodiment, "a secure VPN is established between the user's computer and the secure target site," without any return of DNS records. (*Id.* at 41:5-15.) In still another, "[t]he gatekeeper would establish a VPN between the client and the requested target" before any IP address is returned. (*Id.* at 41:23-32.)

Likewise, in an embodiment relating to Fig. 34, the SDNS only returns a secure URL after it has already coordinated with the VPN gatekeeper to establish a VPN. For example, in step 3409, "SDNS 3313 accesses VPN gatekeeper 3314 for establishing a secure communication link between software module 3309 (on computer 3301) and secure server 3320," and then VPN gatekeeper provisions computer 3301 and secure web server 3320 or its edge router, "thereby creating the VPN." (*Id.* at 51:34-40.) Next, in step 3410, the SDNS 3313 returns a secure URL either through an administrative VPN link or "in the clear," it does not matter which. (*Id.* at 51:44-61.) Then, in step 3411, the software module on computer 3301 "accesses secure server 3320 through VPN communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314." (*Id.* at 51:62-64.)

By comparison, the mere return of requested DNS records, without more, is described in the specification only as a default process for *non-secure communications*. (*Id.* at 40:25-29, "Had the user requested lookup of a non-secure web site . . . , DNS proxy would *merely pass through to conventional DNS server 2609* the look-up request," emphasis added; *see also id.* at 39:56-61, 40:49-56, 41:41-49.) Therefore, the Office's unreasonably broad claim construction improperly encompasses the very conventional and unremarkable features that the '504 patent specification "repeatedly, consistently, and exclusively" distinguishes and disparages. *Abbott*, 696 F.3d at 1150.

The '504 patent claims reinforce the specification's disparagement of the conventional features in the prior art. Many of the claims recite various configurations of a DNS system. These configurations include, for example, a DNS system *configured* to comprise an indication that the DNS system supports establishing a secure communication link. (*See, e.g.*, '504 patent claim 1.) Certain dependent claims are additionally directed to the returning of requested DNS records, which the '504 patent claims as *another configuration*. (*See, e.g.*, *id.* at claim 15, "[t]he system of claim 1, wherein the domain name service system is configured *to provide, in response to the query, the network address corresponding to a domain name*," emphasis added; *see also id.* at claims 14, 16, 35, 38-40, 59.) These query-response claims reflect the specification embodiments that not only support establishing a secure communication link, *but additionally* return an IP address. (*See, e.g.*, *id.* at 40:6-24, 41:23-32.) Thus, the '504 patent's specification and its claims are in harmony regarding the conventional features of returning requested DNS records, such as an IP address or public key. Construing the recited "indication" to include the disparaged and disclaimed conventional features, as the Office has done, is unreasonable in light of the specification and the differentiation in the claims. Indeed, returning requested DNS records indicates nothing more than that a DNS system has merely performed the conventional duties asked of it.

Recognizing that the '504 patent describes IP address or public key messages as conventional features, Requester appears to argue that only explicit, rigid definitions or disclaimers can affect claim scope. (Comments at 18-19.) This is not the law. The Federal Circuit has instructed that the type of "rigid formalism" advocated by Requester is not required to establish a disclaimer:

> Astrazeneca seems to suggest that clear disavowal requires an "expression of manifest exclusion or restriction" in the form of "my invention does not include _____." But again, such rigid formalism is not required: Where the general summary or description of the invention describes a feature of the invention . . . and criticizes other products . . . that lack that same feature, this operates as a clear disavowal of these other products (and processes using these products).

Astrazeneca AB v. Mut. Pharm. Co., 384 F.3d 1333, 1340 (Fed. Cir. 2004) (holding that the patentee's specification "clearly disavow[ed] nonsurfactant solubilizers" by describing, in relation to the invention, micelle structures only formed by surfactant solubilizers, while at the same time criticizing the undesired effects associated with using other types of solubilizers); *see also Abbott*, 696 F.3d at 1148-50 (holding that the broadest reasonable construction of "electrochemical sensor" was one without cables or wires, and that the specification did not need to include an "express disclaimer" of a sensor with cables and wires when every disclosed embodiment was devoid of cables and wires, and the specification only mentioned a sensor with cables or wires to disparage the prior art).

The disclaimers found in the '504 patent far exceed the threshold set by controlling cases and reflect an unmistakable disavowal of claim scope that the Office must respect in its claim-construction analysis. Because the cited references disclose only conventional features that are outside the scope of the properly construed claims, the Office should withdraw the rejections relying on those references and allow all pending claims. If the Office persists in rejecting the claims, the next Office Action should be a nonfinal action setting forth its construction of the disputed claim terms and explaining how its construction applies to each of the cited references for each of the rejected claims. *See* M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed.").

III. The Rejections Based on *Lendenmann* Should Be Withdrawn (Issues 1, 3-5, 7, and 8)

A. The Rejection of Claims 1-3, 5, 6, 14-30, 33-54, and 57-60 Based on *Lendenmann* (Issue 1) Should Be Withdrawn

Claims 1-3, 5, 6, 14-30, 33-54, and 57-60 were rejected under 35 U.S.C. § 102(b) based on *Lendenmann*. (Second OA at 6.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

1. Independent Claim 1

Independent claim 1 recites, among other things, "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." *Lendenmann* fails to disclose this feature for the several reasons discussed below.

a. Bases for the Rejection that Have Been Withdrawn

Patent Owner appreciates the Office's recognition that the "server status" and "online documentation" of *Lendenmann* do not relate to an indication that the domain name service system supports establishing a secure communication link. (*Id.* at 26.) Patent Owner maintains that these bases for the rejection should remain withdrawn for at least the reasons discussed in its Response at 12-15.

b. The Remaining Bases for the Rejection Do Not Disclose the Recited "Indication" as that Term Is Construed by the Office

As discussed above in Section II.C, the Office purports to construe the "indication" recited in claim 1 as "a visible message or signal to a user that the DNS system supports establishing a secure communication link." (*Id.* at 21-22, citing Ex. A to Requester's Comments in control no. 95/001,788.) The Office, however, does not apply its own claim construction to any alleged "indication." For instance, the Office does not explain how the CDS's mere returning of a network address is a "visible message or signal to a user." (*Id.* at 23.) The Office also does not explain how the alleged incorporation of ACL management software into the CDS constitutes a "visible message or signal to a user." (*Id.* at 24-25.) The Office likewise fails to explain how binding handles or authentication challenges constitute a "visible message or signal to a user." (*Id.* at 25.) This is all because *Lendenmann* does not disclose that such features are visible messages or signals *to a user*. (Supp. Keromytis Decl. ¶ 17.) Additionally, one of ordinary skill in the art would not have had reason to visually convey these features to a user in the context of *Lendenmann*'s system. (*Id.*) Thus, for the reasons discussed above in Section II.C, the rejection of claim 1 should be withdrawn.

c. *Lendenmann*'s CDS "Returning a Network Address" Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The Office originally rejected claim 1 over *Lendenmann* on the basis of the CDS merely "returning the network address corresponding to a secure domain name." (OA at 11, incorporating Req. Ex. F-1 at 13.) Rather than rebut Patent Owner's arguments that such a feature is a

conventional and disclaimed feature that does not correspond to the "indication" recited in claim 1, (Response at 7-8), the Office now asserts that Patent Owner fails to take into account the "'numerous secure communications feature *that go beyond* merely resolving a name into a network address' . . . . These features will be discussed *infra*." (Second OA at 23, emphasis added, quoting Comments at 3.)

By changing course and relying now on bases *other than* the mere returning of a network address to maintain the rejection of claim 1 (i.e., those that "go beyond" returning a network address), the Office appears to agree with Patent Owner that the returning of a network address in *Lendenmann* does not disclose an "indication that the domain name service system supports establishing a secure communication link." Accordingly, the rejection of claim 1 on this basis should be withdrawn.

d. *Lendenmann*'s "Access Control List Integrated into the Cell Directory Service" Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The Office asserts that the Access Control List ("ACL") incorporated into the CDS of *Lendenmann* discloses the recited "indication." This is incorrect.

The Office and Requester assert that the CDS *itself* performs access checking based on ACL entries because the ACL software is "incorporated into all CDS clerks and servers." (*Id.* at 24; Comments at 4.) But *Lendenmann* clearly explains that the ACL management software itself performs the checks. (*Lendenmann* 34; Supp. Keromytis Decl. ¶ 18.) And ACLs are a functionality of the DCE Security Service addressed in Chapter 3 ("Security Service") of *Lendenmann*—not the CDS. (*Lendenmann* 41, 62-66, subchapter titled "Access Control List Facility.") Requester admitted as much in its Request when quoting: "The CDS server *only completes an operation over the clearinghouse if the user is authenticated and authorized* by the Security Service." (Req. Ex. F-1 at 14, quoting *Lendenmann* 34, emphasis original.) Accordingly, the Office and Requester are incorrect in their arguments that the CDS itself performs the access-checking, and the rejection should be withdrawn.

Moreover, regardless of whether the ACL is part of the Security Service or part of the CDS, the CDS does nothing more than either return a network address (or binding handle), or not return one. The Office appears to recognize this shortcoming by arguing that certain embodiments in the '504 specification also do nothing more than return a network address, which allegedly corresponds to the "indication" recited in claim 1. But these embodiments do not support the Office's arguments.

For example, the Office cites and quotes from col. 40, ll. 19-24, asserting that the embodiment discussed in this passage does nothing more than return a network address. (Second OA at 25.) But in this embodiment, the return of a network address occurs only *after* the DNS proxy "*transmits a message . . . requesting that a virtual private network be created* between user computer 2601 and secure target site 2604." ('504 patent 40:14-16, emphasis added.) Thus, viewed in proper context, the passage carved out by the Office discloses a DNS system that does more than return a network address: it actively liaises with a gatekeeper device to create a VPN. (*Id.*; Supp. Keromytis Decl. ¶ 20.)

The Office also relies on col. 51, ll. 48-61, which discusses step 3410 of Fig. 34, for the same proposition. (Second OA at 25.) However, the '504 patent discloses that in the immediately preceding step of Fig. 34, the SDNS "accesses VPN gatekeeper 3314 for establishing a VPN communication link." ('504 patent 51:34-46, step 3409.) Only after this, in step 3410, is an address returned in two alternative scenarios: either via an administrative VPN or "in the clear," it does not matter which. (*Id.* at 51:44-61.) Then, in step 3411, the secure server is accessed through the "VPN communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314." (*Id.* at 51:62-64.) By selectively quoting only one portion of step 3410, the Office ignores that this embodiment also does far more than merely return a network address: it actively liaises with gatekeeper 3314 to establish a VPN communication link. (*Id.* at 51:34-36; Supp. Keromytis Decl. ¶ 21.) Accordingly, neither of the DNS system embodiments cited by the Office, when considered in their full context, support the Office's maintained rejection. Thus, the rejection should be withdrawn.

Finally, even when the CDS is supplemented with the functioning of the Security Service's ACL, which simply "defines the access rights of a specific principal (or group) to the object to which the ACL is associated," (*Lendenmann* 63), the CDS merely returns a network address (or binding handle), or fails to return one. This exhausts the CDS's and the ACL's roles. But the return of a network address does not differentiate between conventional systems and systems configured to "comprise an indication that the domain name service system supports establishing a secure communication link," as network addresses are typically returned *in both types of systems*. (Supp. Keromytis Decl. ¶ 22.) Like the CDS, the conventional DNS systems disparaged and disclaimed in the '504 patent specification may also similarly fail to return a network address for one of any number of reasons. (*Id.*) Therefore, the mere returning of a network address (or not returning a network address) does not indicate anything at all about the alleged DNS system in question. As a result, the rejection is improper and should be withdrawn.

Finally, in improperly maintaining the rejection, the Office also asserts that Patent Owner "characterize[s] DNS authorization as a distinguishing inventive feature." (Second OA at 24.) The Office's emphasis on disclosed but unclaimed features is improper and irrelevant. Claim 1 recites "an indication that the domain name service system supports establishing a secure communication link." The Office's analysis lacks any nexus with this claim language, and therefore fails to support the rejection.

For all of the above reasons, the rejection of claim 1 based on the ACL should be withdrawn.

e. *Lendenmann*'s Binding Handles Fail to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

In response to Patent Owner's argument that *Lendenmann*'s binding handles returned by a CDS do not contain any security annotations, the Office argues that "[o]nly well-known endpoints are stored in CDS . . . [i]n this case clients obtain fully bound handles." (*Id.* at 25.) According to the Office, this "fully bound" statement means that the binding handles contain security annotations that allegedly correspond to the "indication" recited in claim 1. (*See id.*) The Office is incorrect.

Lendenmann succinctly defines a "fully bound" binding handle as nothing more than a binding handle with an endpoint. (*See, e.g.*, *Lendenmann* 179.) "The complete address of a server instance is called a fully bound binding handle, and it contains a host address and an endpoint." (*Id.*) Binding handles are often *not* fully bound because DCE permits "servers to dynamically create their own endpoints." (*Id.*) Thus, adding an endpoint to a binding handle is often necessary to render it fully bound. (*Id.*) Contrary to the Office's assertions, whether a binding handle is fully bound has no bearing on whether it has security annotations. (*See id.*) A person of ordinary skill in the art would have understood that a binding handle requires an endpoint in order for it to be used in making a remote procedure call, and that "fully bound" refers to a binding handle that contains an endpoint. (Supp. Keromytis Decl. ¶ 24; *Lendenmann* 179.)

This definition of a "fully bound" binding handle is consistently repeated throughout *Lendenmann*. For example, "[w]hen executing an RPC call with a partly bound handle, the client RPC runtime contacts the remote DCE daemon to obtain the fully bound handle *with an endpoint* to a compatible server." (*Lendenmann* 184, emphasis added.) No security annotations are involved. (*See id.*) The language quoted by the Office in the rejection, within its full context, also clearly explains the simple relationship between endpoints and whether a binding handle is "fully bound":

> Binding information in CDS does not have endpoints; binding handles returned by NSI calls are *partly bound*. Dynamic endpoints can be different every time they are assigned; so information in CDS would have to be updated very frequently if CDS

> were to store *fully bound handles* containing endpoints. Only well-known endpoints are stored in CDS. In this case, clients obtain *fully bound handles*.

(*Id.* at 186.) The language above, relied upon by the Office and Requester, does not support the argument that a fully bound binding handle contains security annotations. (*See* Second OA at 25; Comments at 5; Supp. Keromytis Decl. ¶ 25.) Rather, the Office's and Requester's interpretation of what it means for a binding handle to be "fully bound" is incorrect and contrary to the specific teachings of *Lendenmann* on this topic. Accordingly, the rejection should be withdrawn.

Furthermore, contrary to the Office's position, *Lendenmann* in fact specifies that a client who receives a binding handle must take additional actions to add security annotations to the binding handle. (Supp. Keromytis Decl. ¶ 26.) "If the client wants authenticated RPC, *it needs to annotate the binding handle* with the name of the server principal and the requested security levels." (*Lendenmann* 198, emphasis added.) This passage of *Lendenmann* further directs the reader to the "RPC and Security" subchapter on pages 191-92. (*Id.*) In this subchapter, *Lendenmann* explains that a client who wants to use authenticated RPC must specify the server principal name and establish the authentication service and protection level, which the client does "with a call to rpc_binding_set_auth_info(), *which adds this security information to the server binding handle*." (*Id.* at 191, emphasis added.)

The concluding subchapter on RPC, summarizing the overall RPC process, also explains the security annotations. "*After* the client has the binding handle, *it can add to it* the desired security level for the RPC calls." (*Id.* at 207-08, subchapter "10.8 Putting It All Together".) Thus, the client must take additional actions to add security information to a binding handle once it receives one. This is equally true if the binding handle is received from a CDS, as the exemplary process described in this summary indicates. (*Id.*, "If the client looks up information in CDS . . . .") This is consistent with the rest of *Lendenmann*, which, as discussed above, also describes the need for a client to add security information to a binding handle that it receives. (*See, e.g.*, *id.* at 191, 198.) This includes the passage selectively quoted in Requester's Comments, which, when considered in its full context, actually elaborates *within the very same paragraph* that the "server *adds* the levels of security it[] supports to the handles" and that the client also "*adds* the requested security level and its own identity into the binding handle." (*Compare* Comments at 5 *with Lendenmann* 185, further directing the reader to page 191.)

Neither the Office nor Requester has presented any evidence that *Lendenmann* discloses or suggests that a fully bound binding handle entails security annotations. (Second OA at 25;

Comments at 5.) As a result, the Office's basis for the rejection relies on a misreading of *Lendenmann*, and the rejection should be withdrawn.

f. *Lendenmann*'s Authentication Challenge Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

In the first Office Action, the Office rejected claim 1 because the CDS allegedly sends an authentication challenge in response to a name service query, which in turn allegedly corresponds to "an indication that the domain name service system supports establishing a secure communication link." (OA at 11, incorporating Req. Ex. F-1 at 16, citing *Lendenmann* 194.) Patent Owner traversed the rejection by illustrating that the passage of *Lendenmann* relied upon by the Office and Requester, subchapter "10.4.4 Key Management and Secret Key Authentication," does not in fact involve or mention the CDS in any manner whatsoever, nor any name service queries. (Response at 11-12, discussing *Lendenmann* 193-94). Rather, this portion of *Lendenmann* involves keys and tickets facilitated by the Security Service. (*Id.*)

In response to Patent Owner's arguments, the Office apparently maintains the rejections on the basis of the broad, general statement that "the 'Directory Service' (i.e., CDS) is based upon the RPC foundation." (Second OA at 26.) It is unclear how this vague statement about an "RPC foundation" corresponds to, or otherwise bears any nexus to, the language of claim 1 reciting "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." The rejection is therefore deficient and should be withdrawn. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) ("[U]nless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it . . . cannot anticipate under 35 U.S.C. § 102.").

In support of its argument, the Office quotes an introductory *Lendenmann* chapter on RPC as stating: "This chapter discusses all components involved in the execution of an RPC, including CDS and Security Services access." (Second OA at 26, quoting *Lendenmann* 173.) But the Office relies on this quotation for a meaning contrary to the teachings of *Lendenmann*, apparently trying to illustrate that a CDS communicates with a client via RPC. This quotation's plain language, however, identifies the CDS and the Security Services as mere "components involved in the execution of an RPC"—not a server that communicates via RPC. (*Lendenmann* 173.) Neither the Office nor Requester rely on any *Lendenmann* passage describing a CDS engaging in RPC.

In fact, *Lendenmann* teaches to the contrary. *Lendenmann* expressly differentiates between various types of communications in DCE. *Lendenmann* explains that its "OSF DCE components use three distributed computing models": (1) the client/server model, (2) the remote procedure call model, and (3) the data sharing model. (*Lendenmann* 8-9.) *Lendenmann* illustrates the client/server model as a request/response system of communication:

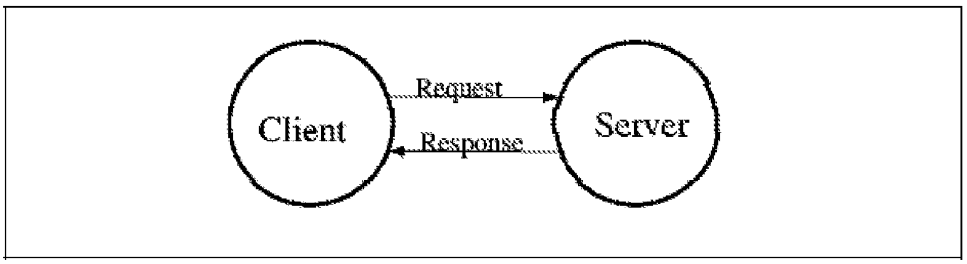


Figure 4. Client/Server Model

(*Id.* at 8.) *Lendenmann* then describes that the CDS "follows the client/server model" just like other DCE applications. (*Id.* at 29.) It specifies that the CDS clerk "receives a request from [a] DCE application." (*Id.*) The CDS clerk then searches for the requested information. (*Id.* at 29-30.) Finally, the clerk "passes the requested data to the client application." (*Id.* at 30.) All of this language is consistent with the client/server model discussed in Figure 4, reproduced above. (*Id.* at 8.) Never is this simple lookup procedure referred to as an RPC.

Accordingly, the Office's and Requester's reliance on broad, general statements outside of their true context is misplaced. These generic statements have no nexus with *Lendenmann*'s express teachings concerning the CDS, and in fact the Office's and Requester's interpretations are contrary to *Lendenmann*'s CDS-specific descriptions. (*See* Second OA at 25-26, quoting *Lendenmann* 173; Comments at 6, same.) Therefore, the Office is incorrect in asserting that an alleged "authentication challenge" corresponds to the "indication" recited in claim 1. The rejection should therefore be withdrawn.

For all of the above reasons, in addition to the reasons set forth in Patent Owner's Response, the rejection of claim 1 should be withdrawn, and its patentability should be confirmed.

2. Independent Claims 36 and 60

Independent claims 36 and 60 include recitations similar to those discussed above in connection with claim 1. Additionally, the Office rejected claims 36 and 60 for the same reasons it rejected claim 1. Thus, for reasons similar to those described above and in the Response with respect to claim 1, *Lendenmann* does not anticipate claims 36 and 60, and the rejections should be withdrawn.

3. Dependent Claims 5, 23, and 47

Claims 5, 23, and 47 each depend from either independent claim 1 or 36, and include all of its features. Accordingly, claims 5, 23, and 47 are patentable for the reasons discussed above with respect to claims 1 and 36, in addition to the reasons discussed below.

The Office maintained the rejection of claims 5, 23, and 47 under the premise that the security service is not separate from the CDS, again arguing that the ACL provides the "authentication" recited in claims 5, 23, and 47. (Second OA at 27, referencing its prior section 3.2.B.) As discussed above in Section III.A.1.d, the Office is incorrect because ACLs are part of the Security Service—not the CDS. (*Lendenmann* 62-66, Security Service subchapter titled "Access Control List Facility.")

Additionally, regardless of whether or not the ACLs are separate from the CDS, the ACLs described in *Lendenmann* do not involve any encryption. (*See, e.g.*, *id.* at 34, 62-66.) Nor do the Office and Requester assert that encryption is involved with the ACLs. Thus, the ACL feature exclusively relied upon by the Office for the rejection in the Second Office Action fails to correspond to a "domain name service system . . . configured to authenticate the query *using a cryptographic technique*," as recited in claim 5 (emphasis added). Thus, the rejection of claim 5 should be withdrawn for this additional reason.

Requester mistakenly argues that communications with a CDS occur via RPC and that the various potential security features of RPC allegedly apply to communications between a client and a CDS. (Comments at 8-10.) Requester is incorrect for at least the reasons discussed above in Section III.A.1.f. Indeed, Requester's misreading of vague, general statements in *Lendenmann* is contrary to the CDS-specific teachings of *Lendenmann*.

For all of the above reasons, in addition to the reasons set forth in Patent Owner's Response, the rejection of claims 5, 23, and 47 is improper and should be withdrawn.

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

Claims 16, 17, 27, 33, 40, 41, 51, and 57 each depend from either independent claim 1 or 36, and include all of its features. Accordingly, claims 16, 17, 27, 33, 40, 41, 51, and 57 are patentable for the reasons discussed above with respect to claims 1 and 36, in addition to the reasons discussed below.

In maintaining the rejection, the Office again argues that the CDS returns more than incomplete bindings. (Second OA at 27.) But as discussed above in Section III.A.1.e, a "fully bound" binding handle is nothing more than a binding handle with an endpoint, and therefore whether a binding handle is "fully bound" or not has no bearing on the features of the claims. (*See,*

e.g., *Lendenmann* 179, 186.) Accordingly, the Office is incorrect for the reasons provided above in addition to the reasons set forth in Patent Owner's Response, and the rejection should be withdrawn.

5. Dependent Claims 24 and 48

Claims 24 and 48 each depend from either independent claim 1 or 36, and include all of its features. Accordingly, claims 24 and 48 are patentable for the reasons discussed above with respect to claims 1 and 36, in addition to the reasons discussed below.

The Office simply labels the arguments in Patent Owner's response "unpersuasive" without addressing their substance, and repeats its prior basis for the rejection. (Second OA at 27; OA at 11, incorporating by reference Req. Ex. F-1 at 37-38.) This is improper in an office action purporting to be an ACP. M.P.E.P. § 2671.02 ("[A]n ACP must . . . include a rebuttal of any arguments raised in the patent owner's response . . . ."). The Comments, meanwhile, suggest nothing more than that a CDS returns a network address when one is requested, which is a conventional feature both disparaged and disclaimed in the '504 patent specification, as discussed above in Section II.C. Accordingly, Patent Owner maintains that the rejection is improper and should be withdrawn for the reasons provided in Patent Owner's Response.

Additionally, rather than substantively responding to the arguments in the Response, the Office contends for the first time in the Second Office Action that claims 24 and 48 are directed to "nonfunctional descriptive material and thus cannot distinguish over the prior art." (Second OA at 28, citing M.P.E.P. § 2106.01.[2]) This is incorrect.

The Office must give claims 24 and 28 their full patentable weight because the claims describe a functional relationship between the "at least one of the plurality of domain names" and the "domain name service system." M.P.E.P. § 2111.05(I)(A) ("To be given patentable weight, the printed matter [i.e., alleged nonfunctional descriptive matter] and associated product must be in a functional relationship. A functional relationship can be found where *the printed matter performs some function with respect to the product to which it is associated*." (emphasis added) (citing *In re Lowry*, 32 F.3d 1579, 1584 (Fed. Cir. 1994))). In claims 24 and 48, the domain name performs a function with respect to the domain name service system on which it is stored—it indicates that the domain name service system supports establishing a secure communication link. The M.P.E.P. provides examples that further illustrate that this claimed relationship is functional:

[2] The Office's reliance on M.P.E.P. § 2106.01 is misplaced. This section addresses subject matter eligibility under 35 U.S.C. § 101, which is outside the permissible scope of *inter partes* reexamination. *See* M.P.E.P. § 2658; 37 C.F.R. § 1.906. Based on the language used in the Second Office Action, Patent Owner submits that M.P.E.P. § 2111.05 provides the proper analysis.

> **A. Evidence For a Functional Relationship**
>
> For instance, indicia on a measuring cup *perform the function* of indicating volume within that measuring cup. . . .
>
> **B. Evidence Against a Functional Relationship**
>
> However, where a product merely serves as a support for printed matter, no functional relationship exists. . . . These situations may arise where the claim as a whole is directed towards conveying a message or meaning to a human reader *independent of the supporting product*. For example, a claimed measuring tape having electrical wiring information thereon . . . *would lack a functional relationship* as the claims as a whole are directed towards conveying wiring information (*unrelated* to the measuring tape) . . . .

M.P.E.P. § 2111.05(I)(A), (B) (emphases added). Like indicia on a measuring cup indicating that the measuring cup stores a particular volume, the domain name stored in the domain name service system indicates that the domain name service system supports establishing a secure communication link. Thus, a functional relationship exists between the "at least one of the plurality of domain names" and the "domain name service system."

Moreover, the Office's apparent requirement that the claim recite a "data structure," (Second OA at 28), has no legal basis. As discussed, the Office must give the claim recitations their full patentable weight when "the printed matter and associated product [are] in a functional relationship. A functional relationship can be found where the printed matter performs some function with respect to the product to which it is associated." M.P.E.P. § 2111.05(I)(A). The M.P.E.P. and the case law impose no such "data structure" requirement. And, as discussed, claims 24 and 48 describe a functional relationship between the "at least one of the plurality of domain names" and the "domain name service system." Thus, the Office must give the claimed features their full patentable weight.

For at least the reasons discussed above, the features recited in claims 24 and 48 must be given their full patentable weight, and *Lendenmann* does not disclose or suggest these features. Accordingly, the rejection of claims 24 and 48 should be withdrawn.

6. Dependent Claims 2, 3, 6, 14, 15, 18-22, 25, 26, 28-30, 34, 35, 37-39, 42-46, 49, 50, 52-54, 58, and 59

Claims 2, 3, 6, 14, 15, 18-22, 25, 26, 28-30, 34, 35, 37-39, 42-46, 49, 50, 52-54, 58, and 59 each depend from either independent claim 1 or 36, and include all of its features. Accordingly, claims 2, 3, 6, 14, 15, 18-22, 25, 26, 28-30, 34, 35, 37-39, 42-46, 49, 50, 52-54, 58, and 59 are patentable for at least the reasons discussed above with respect to claims 1 and 36.

B. The Rejection of Claim 7 Based on *Lendenmann* in View of *Wesinger* (Issue 3) Should Be Withdrawn

The Office maintains the rejection based on its argument that there is no "'separate Security Service' distinct from the CDS." As discussed above in Section III.A.1, the Office is incorrect. Accordingly, the rejection of claim 7 should be withdrawn for the reasons stated in the Response. (Response at 20-21.)

C. The Rejection of Claims 8 and 9 Based on *Lendenmann* in View of *Gaspoz* (Issue 4) Should Be Withdrawn

The Office maintains the rejection based on its argument that there is no "'separate Security Service' distinct from the CDS." As discussed above in Section III.A.1, the Office is incorrect. Accordingly, the rejection of claims 8 and 9 should be withdrawn for the reasons stated in the Response. (*Id.* at 21-23.)

D. The Rejection of Claim 10 Based on *Lendenmann* in View of *Gaspoz* in Further View of *Martin* (Issue 5) Should Be Withdrawn

The Office maintains the rejection based on its argument that there is no "'separate Security Service' distinct from the CDS." As discussed above in Section III.A.1, the Office is incorrect. Accordingly, the rejection of claim 10 should be withdrawn for the reasons stated in the Response. (*Id.* at 23-24.)

E. The Rejection of Claims 12 and 13 Based on *Lendenmann* in View of *Gaspoz* in Further View of RFC 793 (Issue 7) Should Be Withdrawn

To support the rejection of claims 12 and 13, the Office relies on the premise that *Lendenmann* discloses the features recited in claim 1. (*See* Second OA at 30-31.) Accordingly, the rejection of claims 12 and 13 are improper and should be withdrawn for the reasons discussed above with respect to claim 1 and for the reasons in the Response. (Response at 25-26.)

The rejection of claims 12 and 13 are also improper and should be withdrawn because the Office ignores and mischaracterizes Patent Owner's arguments in the Response. For example, the original rejection stated that the features recited in claim 12 are allegedly obvious because "*Lendenmann*'s remote procedure call, which operates over TCP, *uses* a 'moving window of valid values' as indicated by RFC 793." (OA at 11, incorporating Req. Ex. F-1 at 140, emphasis added.) But claim 12 requires more than just "using" a moving window—it requires that the VPN "*is based on* comparing a value in each data packet . . . to a moving window of valid values" (emphasis added).

The Office apparently takes the position that if secure communications run over the TCP protocol, the security features of those communications are thereby "based on" features of the TCP protocol itself. (Second OA at 30; OA at 11, incorporating Req. Ex. F-1 at 140.) This is an

unreasonable position that is irreconcilable with what one of ordinary skill in the art would have understood at the time of the invention. (Supp. Keromytis Decl. ¶ 29.) If true, the Office's position would mean that *all TCP-based communications* are VPNs if they comply with RFC 793, since all of those communications would similarly be "based on" the TCP features purportedly giving rise to a VPN, as stated in the rejection. (Second OA at 30; OA at 11, incorporating Req. Ex. F-1 at 140.) Since the Office's arguments based on RFC 793 are unreasonable and contrary to how a person of ordinary skill in the art would have understood the asserted references, and since the Office provides no other reasoning to show that the additional features of claim 12 are obvious whether in further combination with *Gaspoz* or otherwise, the rejection is improper and should be withdrawn.

Moreover, the Office's rejection of claims 12 and 13 is based on a conclusory obviousness analysis that fails to support the rejection. A rejection based on obviousness "cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Here, the Office overlooks difficulties and limitations with *Gaspoz*, which the Office acknowledges in explaining that "manual file creation rather than object programming is required to create a VPN" in *Gaspoz*. (Second OA at 29.) Given these limitations, a person of ordinary skill would not have looked to combine *Gaspoz* with either *Lendenmann* or RFC 793, and the Office has provided no "articulated reasoning" to the contrary. Thus, the rejection of claims 12 and 13 is improper for this additional reason.

F. The Rejection of Claims 31, 32, 55, and 56 Based on *Lendenmann* in View of *Ludwig* (Issue 8) Should Be Withdrawn

The Office maintains the rejection based on its argument that there is no "'separate Security Service' distinct from the CDS." But as discussed above in Section III.A.1, the Office is incorrect. Accordingly, the rejection of claims 31, 32, 55, and 56 should be withdrawn for the reasons stated in the Response. (Response at 27.)

For all of the above reasons, the rejections based on *Lendenmann* alone and in combination with various references (Issues 1, 3-5, 7, and 8) should be withdrawn, and the claims should be confirmed.

IV. The Rejections Based on *Aziz* Should Be Withdrawn (Issues 9, 11-13, and 15)

A. The Rejection of Claims 1, 2, 6-9, 14-22, 24, 25, 27, 28, 33-46, 48, 49, 51, 52, and 57-60 Based on *Aziz* (Issue 9) Should Be Withdrawn

Patent Owner appreciates the Office's recognition that the rejection of claims 5, 23, 47, and 50 has been withdrawn,[3] and Patent Owner maintains that those rejections should remain withdrawn at least for the reasons provided in the Response. However, the Office maintains its rejection of claims 1, 2, 6-9, 14-22, 24, 25, 27, 28, 33-46, 48, 49, 51, 52, and 57-60 under 35 U.S.C. § 102(e) based on *Aziz*. (Second OA at 12.) For at least the reasons discussed in the Response and discussed below, these rejections should be withdrawn and the claims should be confirmed.

1. Independent Claim 1

Independent claim 1 recites, among other things, "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." As explained above in Section II, the rejections are based on improper claim constructions. In particular, the Office relies upon an unreasonably broad and erroneous construction of the claimed DNS system that renders the rejections improper. Additionally, the Office construes the "indication" recited in claim 1 but never applies that construction to the alleged indications, leaving Patent Owner no opportunity or basis on which to challenge the rejection. Finally, the Office asserts that four different portions of *Aziz* disclose the recited "indication": (1) returning the address of a firewall via an SX record; (2) returning public keys and digital signatures of the firewall via KEY and SIG records; (3) building tunnel information tables using the SX, KEY, and SIG records; and (4) *Aziz*'s reference to DNS-sec and RFC 2065. The Office is incorrect.

a. *Aziz*'s Authorized Client 210 Is Not a DNS System Component

In the *Aziz* rejections, the Office criticizes Patent Owner for "incorrectly characteriz[ing] the incorporated rejection as limit[ing] the claimed 'domain name service system' to Name Server (NS) 120." (Second OA at 31.) The Office's criticism is misplaced. To the extent Patent Owner focused on the NS 120 in its Response, Patent Owner did so because the allegations before it at the time of the First Office Action also focused on the NS 120. For example, as Patent Owner explained in the Response, while the Request initially appeared to take the unreasonable position that *everything* in Fig. 1 of *Aziz* could be included in the alleged DNS system, the Request's proposed rejection of

[3] While the Office indicates that the rejection of claims 5, 23, ***27***, and 50 have been withdrawn, (Second OA at 4, 38, and 41), Patent Owner believes that the Second Office Action contains a typographical error and understands that the rejections of claims 5, 23, ***47***, and 50 have been withdrawn. In particular, claims 5, 23, and 47 were argued together because *Aziz* does not disclose authenticating a query for a network address. (Response at 34-35.) Claim 47, and not claim 27, includes this feature.

claim 1, as a whole, focused on name server 120. (Response at 28-29.) Then, as Patent Owner explained, the First Office Action ultimately took the position that NS 120 was the alleged DNS system. (*Id.* at 29.)

Moreover, Requester's Comments mischaracterize the position taken in the Response, claiming that "Patent Owner asserts that the claimed 'domain name service system' must be embodied in a single *server*, not in a 'system' that may be comprised of multiple components." (Comments at 18, citing Response at 28-29.) Patent Owner never made such an argument. Instead, Patent Owner simply asserted that Requester could not reasonably assert that *everything* in Fig. 1 of *Aziz* was included in the alleged DNS system. (Response at 28-29.) Indeed, as discussed above in Section II.B, the Office's unbounded claim construction of this term is improper. Patent Owner, when considering the positions of the Request and Office Action as a whole, simply responded to the rejection based on the Office Action's stated position that the NS 120 is the recited DNS system. (*Id.* at 29.)

In the Second Office Action, the Office expands its interpretation of DNS system with respect to *Aziz*. The Office now contends that authorized client 210 is also part of the DNS system along with NS 120. (*See, e.g.*, Second OA at 32, "The DNS system comprises authorized client 210 . . . .") Having squeezed authorized client 210 into its interpretation of a DNS system, the Office now asserts that "[t]he DNS system thus supports establishing a secure communication link," and relies on this overly broad interpretation of a DNS system with regard to three of the alleged "indications" disclosed by *Aziz*: (1) returning the address of a firewall via an SX record; (2) returning public keys and digital signatures of the firewall via KEY and SIG records; and (3) building tunnel information tables using the SX, KEY, and SIG records. However, authorized client 210 cannot be reasonably considered a part of the alleged DNS system, and thus the Office's positions with regard to these alleged indications fail.

The Office's rationale for why authorized client 210 is a part of the alleged DNS system is because it includes a resolver program that "(1) return[s] the answer to the query if it is available locally; otherwise, (2) find[s] the best servers to ask for the answer; (3) send[s] queries to the servers until one response; and (4) process[es] the response." (*Id.*, quoting *Aziz* 7:3-7.) Thus, *Aziz* discloses a conventional client-based resolver program that merely sends out a DNS query on behalf of application programs co-located at the authorized client, processes the DNS response received as a result of its query, and possibly caches the response locally in order to minimize the number of queries it has to send to name servers. (Supp. Keromytis Decl. ¶ 30.)

But this relationship—based on querying an alleged DNS system—does not transform authorized client 210 into a part of the alleged DNS system itself. (*Id.*) Indeed, if merely sending and receiving DNS queries qualified a network component as being a part of the alleged DNS system, then literally any network component (e.g., a client, user-agent, firewall, proxy, edge router, etc.) that can communicate over a network would be a part of the alleged DNS "system." (*Id.*) This expansive interpretation is not supported by the '504 patent, as discussed above. (*See supra* Section II.B; *see also* Supp. Keromytis Decl. ¶ 30.)

Because the Office's positions with respect to the first three alleged "indications"—returning a firewall network address, returning keys and signatures, and building tunneling information tables—rests on its improper construction of a domain name system, each of those positions fails. Nonetheless, when addressing these alleged "indications" in the subsections below, Patent Owner assumes, solely for the sake of argument, that authorized client 210 may properly be included as a part of the alleged DNS system, even though it cannot.

b. *Aziz* Does Not Disclose the Recited "Indication" as that Term Is Construed by the Office

As discussed above in Section II.C, the Office interprets the "indication" recited in claim 1 as "a visible message or signal to a user that the DNS system supports establishing a secure communication link." (Second OA at 21-22, citing Comments in control no. 95/001,788, Ex. A.) The Office, however, does not apply its own construction of this term when addressing *Aziz*. For example, the Office does not explain how any one of the four alleged "indications" in *Aziz*—(1) returning the address of a firewall via an SX record; (2) returning public keys and digital signatures of the firewall via KEY and SIG records; (3) building tunnel information tables using the SX, KEY, and SIG records; and (4) *Aziz*'s reference to DNS-sec and RFC 2065—is a "*visible* message or signal *to a user.*" (*See id.* at 31-38, emphases added.) This is because *Aziz* does not disclose that any of these alleged "indications" are visible messages or signals to a user. (Supp. Keromytis Decl. ¶ 31.) Thus, because the Office does not demonstrate how *Aziz* discloses an "indication" as the Office interprets the term, the rejection of claim 1 is legally deficient and cannot support a finding that *Aziz* anticipates the claim. For at least these reasons and those discussed above in Section II.C, the rejection of claim 1 should be withdrawn.

c. *Aziz*'s Returning the Address of a Firewall Via an SX Record Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

As explained in the Response, *Aziz*'s returning the address of a firewall via an SX record does not disclose the recited "indication that the domain name service system supports establishing a secure communication link." (Response at 29-30.) The Office disagrees and asserts that: (1) authorized client 210 is a part of the DNS system and "directly establishes a secure communication with the target"; and (2) even if authorized client 210 is not a part of the DNS system, *Aziz* teaches that "releasing the address of firewall 110 (SX record) provides an indication . . . ." (Second OA at 32.) The Office is incorrect on both points.

First, even assuming *arguendo* that authorized client 210 is a part of the DNS system, which it is not, (*see supra* Section IV.A.1.a), returning the address of firewall 110 via an SX record does not indicate anything about the capabilities of authorized client 210 (Supp. Keromytis Decl. ¶ 32). And returning the address of firewall 110 certainly does not indicate that authorized client 210 supports establishing a secure communication link. (*Id.*) For example, *Aziz* discloses that when NS 120 receives a query for a host address, determines whether an SX record exists for the corresponding host name. (*Aziz* 9:49-53.) If one exists, NS 120 adds the SX record to the response. (*Id.* at 9:53-55.) Thus, the SX record is returned to authorized client 210 based merely on whether the SX record exists for a particular host name, and regardless of whether authorized client 210 supports establishing a secure communication link. (Supp. Keromytis Decl. ¶ 32.) Accordingly, even if authorized client 210 is incorrectly considered to be a part of the alleged DNS system, returning an SX record still does not indicate that the alleged DNS system supports establishing a secure communication link.

Second, the Office's assertion that merely releasing the address of firewall 110 via the SX record provides the recited indication relies on an interpretation of "indication" that is unreasonably broad in light of the '504 specification. As discussed above in Section II.C, the broadest reasonable interpretation of the recited "indication," when read consistent with the specification, does not include merely returning requested resources, e.g., IP addresses. The Office cannot construe the recited indication to cover configurations that the specification disparages as conventional and disclaims.

Indeed, Requester's own expert agreed in a copending litigation involving the '504 patent that NS 120 is a conventional server that responds to DNS queries in a conventional manner:

> Q. Is outside NS 120 a server? a computer? Is it a mobile phone? *What -- what type of hardware is outside NS 120?*
>
> A. Well, it's -- I believe it's described as a server, which I would understand is not a mobile phone, although mobile phones are pretty powerful, they could be servers. But it's -- ***it's a conventional server*** which contains DNS application functionality.
>
> . . .
>
> Q. And can you identify what it is in your analysis where you specifically called out what is the determining step in Aziz?
>
> * * *
>
> A. Certainly. Well, starting on page 17 there's a discussion that as a registered DNS server -- that's NS 120 -- that contains additional resource records for some domain names and these additional records may be provided as part of the response message to a DNS request from a client.
>
> The request -- the response can contain additional records that are of type SX, SIG, S-I-G, and KEY. And those records, when they're present, they're used for setting up a secure communication between the gateway and the client computer.
>
> And the discussion indicates the DNS server can be configured to return SX record. It doesn't have to have SX records for particular domain names. ***It responds to requests from users from outside the firewall in a conventional manner.*** It can contain optional resource records to support secure server connections. And once the Authorized Client receives such SX records, the additional records, KEY records, it can set up a secure encrypted communication link. So that's discussed on page 18.

(Ex. A-13 at 166:6-13, 168:23-169:22, emphases added.)

Thus, Requester's own expert agrees that NS 120 does nothing more than conventionally respond to DNS queries by returning whatever relevant records it has. NS 120 does nothing more. Therefore, NS 120 merely returning network addresses and keys in a manner that both the '504 patent specification and Requester's own expert describes as conventional cannot be the recited indication that the DNS system supports establishing a secure communication link.

d. *Aziz*'s Returning Public Keys and Digital Signatures of the Firewall Via KEY and SIG Records Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

As explained in the Response, *Aziz*'s returning public keys and digital signatures of the firewall via KEY and SIG records also does not disclose the recited indication. (Response at 31-32.) The Office again disagrees and asserts that: (1) authorized client 210 is a part of the DNS system and "directly establishes a secure communication with the target"; and (2) even if authorized client 210 is not a part of the DNS system, *Aziz* teaches that the DNS system still provides an indication by releasing the KEY and SIG records. (Second OA at 35.) The Office is incorrect on both points.

First, for similar reasons discussed in the section above regarding SX records, even assuming *arguendo* that authorized client 210 is a part of the DNS system, returning KEY and SIG records does not indicate anything about the capabilities of authorized client 210, and certainly does not indicate that authorized client 210 supports establishing a secure communication link. (Supp. Keromytis Decl. ¶ 33.) For example, *Aziz* discloses that when sending the SX record, NS 120 may also send corresponding KEY and SIG records. (*Aziz* 9:34-40, 10:1-5.) But, again, *Aziz* discloses returning the SX record (and thus the KEY and SIG records) based merely on whether one exists for a particular host name, and regardless of whether authorized client 210 supports establishing a secure communication link. (Supp. Keromytis Decl. ¶ 33.) Accordingly, even if authorized client 210 is incorrectly considered to be a part of the alleged DNS system, returning KEY and SIG records still does not indicate that the alleged DNS system supports establishing a secure communication link.

Second, the Office's assertion that returning KEY and SIG records corresponds to the recited indication relies on an interpretation of "indication" that is unreasonably broad in light of the '504 patent specification. As discussed above in Section II.C, the broadest reasonable interpretation of the recited "indication," when read consistent with the specification, does not include merely returning requested resources, such as IP addresses and public keys. The Office cannot construe the recited indication to cover configurations that the specification disparages and disclaims.

The Office asserts that returning KEY and SIG records "in *Aziz* [is] hardly directed to a 'conventional DNS system.'" (Second OA at 37.) First, as discussed above, even Requester's expert disagrees and has stated that NS 120 "responds to requests from users from outside the firewall in a conventional manner." (Ex. A-13 at 168:23-169:22.) Second, the paragraph immediately following the portion of *Aziz* that the Office cites to allegedly support its position, (Second OA at 36, citing *Aziz* 5:62-6:10), explains that RFC 2065 describes an exemplary embodiment of using KEY and SIG records. (*Aziz* 6:11-15, citing RFC 2065.) RFC 2065, however, was replaced and made obsolete by RFC 2535, which the '504 patent distinguishes as a "conventional scheme." (*See* Ex. A-6 at 1, 44-45; *see also* '504 patent 39:34-41, "One *conventional scheme* that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. . . . One implementation of this standard is presently being developed as part of the FreeS/WAN project (*RFC 2535*)," emphases added.) The '504 patent's disparaging of RFC 2535 as conventional applies equally to RFC 2535's predecessor, RFC 2065. As such, *Aziz*'s conventional key architectures cannot show the "indication" recited in the claims because the broadest reasonable interpretation of the term cannot include such architectures as the

'504 patent distinguishes its embodiments from these types of implementations. *See, e.g.*, *Abbott*, 696 F.3d at 1149-50.

e. *Aziz*'s Building Tunnel Information Tables Using the SX, KEY, and SIG Records Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

As explained in the Response, *Aziz*'s building tunnel information tables using the SX, KEY, and SIG records also does not disclose the recited "indication" limitation. (Response at 32-33.) The Office again disagrees and asserts that Patent Owner's arguments are based on an incorrect assertion that authorized client 210 is not part of the DNS system. (Second OA at 37.) Instead, the Office asserts that authorized client 210 is a part of the DNS system and "directly establishes a secure communication with the target." (*Id.*) Thus, according to the Office, the DNS system (including authorized client 210) provides an indication that it supports establishing a secure communication link by building tunnel information tables necessary for a secure connection. (*Id.* at 37-38.) This is incorrect.

First, as discussed above, the Office is incorrect that authorized client 210 can reasonably be a part of the alleged DNS system. The Office's entire rationale for why *Aziz*'s building tunnel information tables discloses the recited indication is premised on the Office's incorrect assumption to the contrary. Thus, because authorized client 210 cannot be a part of the alleged DNS system, this analysis is likewise improper.

Moreover, even assuming *arguendo* that authorized client 210 is a part of the alleged DNS (which it is not), *Aziz*'s building tunnel information tables does not disclose the recited indication. Patent Owner understands that what the Office refers to as "tunnel information tables" are the disclosed "tunnel maps" of *Aziz*. But, *Aziz* makes clear that the tunnel maps merely store the "destination and secure exchanger addresses[] and related cryptographic data (e.g., secure exchanger's key or algorithm." (*Aziz* 7:28-38; *see also id.* at Fig. 5.) In other words, the tunnel map includes the A, SX, KEY, and SIG records received by authorized client 210 from NS 120. (Supp. Keromytis Decl. ¶ 34.) Patent Owner has already explained that sending and receiving these records are conventional features that are distinguished and disparaged by the '504 specification. Again, the Office cannot construe the recited indication to cover configurations that the specification disparages and disclaims.

f. *Aziz*'s Reference to RFC 2065 and DNS-sec Fails to Disclose an "Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The Office also incorrectly asserts that *Aziz*'s reference to RFC 2065 and DNS-sec discloses the recited indication. (Second OA at 38.) The Office advances two reasons why this portion of *Aziz* allegedly discloses this feature. Each is incorrect.

First, the Office asserts that "*Aziz* teaches the security extension to DNS ('DNS-sec') (RFC 2065) in one embodiment is used to distribute the KEY and SIG records." (Second OA at 38.) As discussed above, however, merely returning the KEY and SIG records cannot be the recited indication and is indeed a conventional feature that is distinguished and disparaged by the '504 patent specification. Moreover, as discussed above, the '504 patent's disparaging of RFC 2535 as conventional applies equally to RFC 2065, which preceded and was made obsolete by RFC 2535.

Second, the Office argues that "the 'assertion that the host speaks IPSEC' bit in the KEY record would provide an indication of support for the establishment of secure communication with the host." (*Id.*) This is incorrect for several reasons. First, RFC 2065 makes clear that Bit 8 in a given KEY record, the bit to which the Office refers: (1) "indicates that *this key is valid for use in conjunction with* [IPSEC]"; and (2) "is an assertion that *the host speaks* IPSEC." (RFC 2065 12, emphases added.) Merely stating that *a key is valid for use* with a particular security protocol, however, does not indicate that a domain name service system *supports establishing* a secure communication link. (Supp. Keromytis Decl. ¶ 35.) Likewise, an assertion that *a host speaks* using a particular security protocol does not indicate that a domain name service system *supports establishing* a secure communication link. (*Id.*) Second, RFC 2065's Bit 8 of a KEY record is merely a part of the very KEY record that the '504 patent disparages as conventional. As Patent Owner explained in the Response, if the KEY record in its entirety cannot include the recited indication because it is conventional, then a single bit within that same KEY record likewise cannot include the recited indication. (Response at 33-34.) The Office's assertion that "this [is] not true as a matter of logic" is simply illogical. Moreover, as Patent Owner has explained, RFC 2535, which the '504 patent specification describes as conventional, succeeds and makes obsolete the RFC 2065 reference that the Office relies on here. In fact, RFC 2535 describes a Bit 4 similar to the Bit 8 described in RFC 2065 that similarly "indicates that this key is valid for use in conjunction with [Oakley/IPSEC]" and "is an assertion that the host speaks Oakley/IPSEC." (Ex. A-6 at 12-13.) The '504 patent's disparaging of RFC 2535 as conventional equally applied to its predecessor, RFC 2065.

In view of the above, *Aziz* does not disclose "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," and thus cannot anticipate claim 1.

2. Independent Claims 36 and 60

Independent claims 36 and 60 include recitations similar to those discussed above in connection with claim 1. Additionally, the Office rejected claims 36 and 60 for the same reasons it rejected claim 1. Thus, for reasons similar to those described above and in the Response with respect to claim 1, *Aziz* does not anticipate claims 36 and 60, and the rejections should be withdrawn.

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

As discussed above with regard to independent claims 1, 36, and 60, *Aziz* does not disclose the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because *Aziz* does not describe such a recited domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, *Aziz* cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or a domain name service system that is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

4. Dependent Claims 18 and 42

Claim 18 recites that "at least one of the plurality of domain names is reserved for secure communication links." *Aziz* does not disclose this feature. In responding to Patent Owner's arguments, the Office asserts that a host inside protected zone 180 of *Aziz* corresponds to a domain name, such as eng.sun.com, and thus concludes that such domain names "are reserved to a protected zone for the possibility of secure communications with an outside, authorized client, *although certainly the initiator is not required to then establish a secure communication link (i.e., take advantage of the reserved domain name*." (Second OA at 39-40, emphasis added.) Thus, the Office eviscerates the meaning of the claim language by asserting that the domain names that are allegedly "reserved" for secure communication links need not be used for secure communication links. (*Id.*) This contradicts the plain meaning of the term "reserved" and does not comport with the understanding of domain names that are reserved for secure communication links in the context of the '504 patent. Indeed, one of ordinary skill in the art would understand that a domain name *reserved* for secure communication links cannot be used for non-secure communication links.

(Supp. Keromytis Decl. ¶ 36.) Instead, the Office departs from the plain meaning of the term "reserved" to effectively rewrite claim 18 to recite that "at least one of the plurality of domain names ~~is reserved~~ can be used for secure communication links." Because the Office's interpretation of the language of claim 18 is unreasonably broad, the rejection should be withdrawn. Claim 42 recites similar features to claim 18 and is also allowable for similar reasons.

5. Dependent Claims 24 and 48

For at least the reasons discussed in the Response, *Solana* does not disclose or suggest that "at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link," as recited in claim 24 and similarly recited in claim 48. Rather than substantively responding to the arguments in the Response, the Office contends that claims 24 and 48 are directed to "nonfunctional descriptive material and thus cannot distinguish over the prior art." (Second OA at 40.) Given this lack of substantive discussion, Patent Owner therefore understands that the Office has determined that *Aziz* does not disclose the additional features recited in claims 24 and 48, and the record should be clarified to state as such.

Moreover, as discussed above in Section III.A.5, the Office must give the features of claims 24 and 48 their full patentable weight because claims 24 and 48 describe a functional relationship between the "at least one of the plurality of domain names" and the "domain name service system." Accordingly, for at least the reasons discussed above and in the Response, the rejection of claims 24 and 48 should be withdrawn.

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

Claims 2, 6-9, 14-15, 19-22, 25, 28, 34, 35, 37-39, 43-46, 49, 52, 58, and 59 each depend from either independent claim 1 or 36, and include all of its features. Accordingly, claims 2, 6-9, 14-15, 19-22, 25, 28, 34, 35, 37-39, 43-46, 49, 52, 58, and 59 are patentable for at least the reasons discussed above with respect to claims 1 and 36.

In view of the above, the rejection of claims 1, 2, 6-9, 14-22, 24, 25, 27, 28, 33-46, 48, 49, 51, 52, and 57-60 in view of *Aziz* should be withdrawn.

B. The Rejection of Claims 3, 4, and 26 Based on *Aziz* in View of *Lawton* (Issue 11) Should Be Withdrawn

Claims 3 and 4 each depend from independent claim 1 and include all of its features. Accordingly, claims 3 and 4 are patentable at least for the reasons discussed above with regard to independent claim 1, and because *Lawton* does not make up for the above-noted deficiencies of *Aziz* with regard to claim 1.

Claim 26 recites that "at least one of the plurality of domain names enables establishment of a secure communication link." The Office advances two arguments why the alleged combination of *Aziz* and *Lawton* discloses this feature. Each is incorrect.

First, the Office asserts that *Aziz* alone teaches that a domain name enables establishment of a secure communication link by returning SX, KEY, and SIG records, which the Office asserts are used for establishing a secure communication link, in response to a domain name query. (Second OA at 42, "Thus, in *Aziz* a domain name enables establishment of a secure communication link.) This argument is entirely new, and thus warrants withdrawal of the Office's ACP designation of its latest Office Action. (*Compare id. with* Req. Ex. F-2 at 88-89.) Further, and more importantly, the argument is incorrect. Returning SX, KEY, and SIG records in response to a domain name query discloses absolutely nothing about the capabilities of the domain name itself, let alone that the domain name enables establishment of a secure communication link.

Second, the Office cites to Requester's comments, arguing that "[t]he requester relied upon *Lawton* to teach publication of a protected domain name so that the domain name would obviously be used [to] enable a secure communication from outside the protected network." (Second OA at 42, citing Comments at 27-28.) Requester argued no such thing. Instead, Requester relied on *Lawton* to teach two things: (1) "[c]reating an 'alternative domain name server' so that business can 'establish your own top-level domain,'" and (2) "[a]lternate DNS extensions could include '.med, .xxx and .ltd' top-level domains." (Comments at 27, citing *Lawton* 1.) Neither portion of *Lawton*, however, discloses "publication of a protected domain name" or using the protected domain name to "enable a secure communication from outside the protected network," as asserted by the Office. More importantly, neither makes up for the above-noted deficiency of *Aziz*. That is, neither portion of *Lawton* discloses a domain name that "enables establishment of a secure communication link."

Requester disparages Patent Owner's Response for allegedly "attacking references individually." (Comments at 27.) Patent Owner has not done so, and has instead repeatedly insisted that "*Aziz* and *Lawton*, alone or in combination, do not disclose or suggest" this feature. (Response at 40, 42.) Moreover, Requester's argument is not only inaccurate, but also flawed. Instead of "clear[ly] articulat[ing] . . . the reason(s) why the claimed invention would have been obvious" in view of the teachings of *Aziz* and *Lawton*, Requester's obviousness argument is conclusory and lacks any rational underpinning. M.P.E.P. § 2142. For example, Requester states: "Accordingly, *Aziz* and *Lawton* teach (i) using a domain name to refer to a protected zone of computers; (ii) providing secure access to the protected zone of computers; and (iii) using specialized domain names to refer to computers." (Comments at 27.) Noticeably missing from these alleged teachings is any disclosure

or suggestion of a domain name enabling establishment of a secure communication link. Yet in the very next sentence, the Requester summarily concludes: "Thus, it would have been obvious that a domain name 'enables establishment of a secure communication link.'" (*Id.*) This falls far short of establishing a prima facie case of obviousness for claim 26. M.P.E.P. § 2142.

In view of the above, the rejection of claims 3, 4, and 26 is improper and should be withdrawn.

C. The Rejection of Claim 9 Based on *Aziz* in View of *Franaszek* (Issue 12) Should Be Withdrawn

The rejection of claim 9 should be withdrawn at least for the reasons stated in the Response. The Office does not substantively address Patent Owner's arguments that the combination of *Aziz* and *Franaszek* does not disclose or suggest the feature recited in claim 9. (*See* Response at 43, subsection a.) For this reason alone, the rejection should be withdrawn.

Moreover, the Office improperly dismisses Patent Owner's argument that *Franaszek* is nonanalogous art. In the Response, Patent Owner asserted that *Franaszek* is nonanalogous art because it is not reasonably pertinent to the problem solved by the claims, namely, enabling secure communications easily and conveniently. (*Id.* at 45-46.) The Office asserts that this argument "is unpersuasive" because enabling secure communications easily and conveniently "is not claimed, and thus the patent owner's arguments are essentially directed to unclaimed features." (Second OA at 43.) This is not the law. The Office must consult not just the claims, but the entire '504 *specification* to determine *the problem that the inventor was trying to solve* when inventing what is claimed: "In determining whether a reference is reasonably pertinent, an examiner should consider *the problem faced by the inventor*, as reflected—either explicitly or implicitly—*in the specification*." M.P.E.P. § 2141.01(a)(I) (emphases added); *see also In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992). Here, the '504 specification clearly sets forth that one of the problems faced by the inventors and solved by the '504 patented inventions is enabling secure communications quickly and easily. (*See, e.g.*, '504 patent 1:30-8:6.) As discussed in the Response, *Franaszek* is not reasonably pertinent to solving this problem and is thus nonanalogous art. The Office incorrectly dismissed this argument. Accordingly, the rejection of claim 9 based on *Aziz* in view of *Franaszek* is improper and should be withdrawn.

D. The Rejection of Claim 10 Based on *Aziz* in View of *Schneier* (Issue 13) Should Be Withdrawn

The Office maintains the rejection of claim 10 based on *Aziz* in view of *Schneier*. This rejection should be withdrawn for the reasons stated in the Response. (Response at 46.)

E. The Rejection of Claims 29-32 and 53-56 Based on *Aziz* in View of *Ludwig* (Issue 15) Should Be Withdrawn

The Office maintains the rejection of claim 29-32 and 53-56 based on *Aziz* in view of *Ludwig*. This rejection should be withdrawn for the reasons stated in the Response. (*Id.* at 49.)

V. The Rejections Based on *Kiuchi* and *Pfaffenberger* Should Be Withdrawn (Issues 16-18, 20, and 21)

A. The Rejection of Claims 1-4, 6, 8, 9, 14-19, 22, 24-30, 33, 34, 36-43, 46, 48-54, and 57-60 Based on *Kiuchi* and *Pfaffenberger* (Issue 16) Should Be Withdrawn

The Second Office Action rejects claims 1-4, 6, 8, 9, 14-19, 22, 24-30, 33, 34, 36-43, 46, 48-54, and 57-60 under 35 U.S.C. § 103 over *Kiuchi* in view of *Pfaffenberger*. (Second OA at 16.) The Office relies heavily on the Requester's positions relating to *Kiuchi* to support this rejection. However, many of Requester's positions were flatly rejected in the underlying *VirnetX v. Apple* litigation, where, after a six-day trial, the '504 patent was found valid over *Kiuchi.* Thus, for at least the reasons discussed below, and for those in Patent Owner's previous Response, the *Kiuchi-Pfaffenberger* rejections should be withdrawn and the claims confirmed as patentable.

1. Independent Claim 1

In all of the *Kiuchi-Pfaffenberger* rejections, the Office maintains its position that *Kiuchi* discloses the claimed DNS system configured to comprise an indication that the DNS system supports establishing a secure communication link, as recited in the independent claims. (*See generally id.* at 45-48.) In particular, the second Office Action contends that *Kiuchi* discloses the claimed "indication that the DNS system supports establishing a secure communication link" (hereinafter "indication") by the C-HTTP name server "releasing the public key, nonce value, and IP address of the secured, server-side proxy." (*Id.* at 45.) The rejections are defective, however, because they are founded on an incorrect construction of the claimed "indication." The Office purports to construe the claimed "indication," but then never applies it to the alleged "indications" in its *Kiuchi* obviousness analysis. Regardless, as explained below, the alleged "indications" in *Kiuchi* do not meet the Office's stated construction. Additionally, rather than applying its stated construction in the rejections themselves, the Office applies a construction that is unreasonably broad and inconsistent with the '504 patent specification, insisting that the above characteristics of *Kiuchi*'s C-HTTP name server disclose the claimed "indication," even though the '504 patent expressly identifies and disclaims such characteristics as conventional of a DNS system.

a. The Office Does Not Apply Its Construction of "Indication" to the Alleged Indications in *Kiuchi*

According to the Office, the claimed "indication" means "a visible message or signal to a user that the DNS system supports establishing a secure communication link." (*Id.* at 21-22.) However, the Office never applies this construction to the alleged "indications" in its analysis of the cited art. For instance, while the Office asserts that *Kiuchi* discloses the claimed "indication" limitations because the C-HTTP name server provides a public key, IP address, and nonce value, the Office does not attempt to demonstrate how *Kiuchi*'s public key, IP address, and nonce value provide a "visible message or signal to a user that the DNS system supports establishing a secure communication link." (*See id.* at 45-48.) As a result, the *Kiuchi* rejections are uninformative and do not establish a prima facie case of unpatentability, and thus should be withdrawn. (*See supra* Section II.C.)

Moreover, the public key, IP address, and nonce value of *Kiuchi*'s C-HTTP name server do not satisfy the Office's unapplied construction of the claimed "indication" limitations. *Kiuchi* does not teach that any of these items are conveyed to a user in the form of a visible message or signal. (Supp. Keromytis Decl. ¶ 38.) Although these items are used by the client-side and server-side proxies in the C-HTTP link, they are not revealed to the user. (*See, e.g.*, *Kiuchi* 66-67; Supp. Keromytis Decl. ¶ 38.) One of ordinary skill in the art would have had no reason to do so. Regardless, even if *Kiuchi* did visually convey the public key, IP address, or nonce value to the user (which it does not), the user would not necessarily understand what they meant. (Suppl. Keromytis Decl. ¶ 38.) Thus, they would not tell "[the] user that the DNS system supports establishing a secure communication link," as required by the Office's construction.

For at least these reasons, the *Kiuchi* rejections should be withdrawn because, even under the Office's construction of the term, *Kiuchi*'s C-HTTP name server is not configured to comprise the claimed "indication."

b. The Office's Position that the Public Key of the Server-Side Proxy in *Kiuchi* Corresponds to the Claimed "Indication" Is Unreasonable and Inconsistent with the Specification

As explained in Patent Owner's prior Response, the '504 patent clearly explains that a DNS system that returns a requested public key was conventional at the time of the inventions. (*See, e.g.*, Response at 51-52.) Indeed, the '504 patent expressly disparages this conventional DNS system characteristic and explains that the claimed DNS configured to comprise an "indication" is directed at addressing drawbacks associated with such conventional DNS systems. (*See supra* Section II.C.)

But the Office ignores this express disclaimer in the '504 patent and insists that *Kiuchi*'s C-HTTP name server returning the public key of the server-side proxy corresponds to the claimed indication. (*See* Second OA at 45-46.) According to the Office, "prior art may anticipate or render obvious a broadly claimed invention regardless of whether the prior art describes 'conventional' technology." (*Id.* at 47.)

The Office misses the point. The return of a public key is not just *any* conventional technology as the Office contends, but a technology that the '504 patent specification specifically targets and disclaims. (*See supra* Section II.C.) As a result, the Office's interpretation that *Kiuchi*'s public key meets the claimed "indication" limitations is plainly inconsistent with how the '504 patent specification describes the claimed subject matter and is therefore improper. "During reexamination, claims are given the broadest reasonable interpretation *consistent with the specification* . . . ." M.P.E.P. § 2258(I)(G) (emphasis added). The Office does not attempt to distinguish *Kiuchi*'s return of a public key from the '504 patent's disclaimer—it simply ignores the disclaimer while insisting that the public key discloses the claimed "indication." (*See* Second OA 45-47.) But under a proper construction consistent with the '504 patent specification, the inventions are not so "broadly claimed" as the Office contends.[4]

Because the Office's interpretation of the claimed "indication" contradicts the express disclaimers made in the '504 patent, the *Kiuchi* rejections are based upon unreasonably broad constructions. The Office cannot construe the recited indication to cover configurations that the specification disparages and disclaims—the return of a public key and the return of an IP address. Accordingly, the *Kiuchi* rejections should be withdrawn and the claims confirmed as patentable.

Additionally, as explained in Patent Owner's response, *Kiuchi*'s public key of the server-side proxy includes no information about the capabilities of the C-HTTP name server—which the Office points to as the alleged DNS system—in terms of establishing a secure communication link. (Response at 51-52; *see* Second OA at 46, "the DNS system (comprising the C-HTTP name server).") The public key disclosed by *Kiuchi* is nothing more than a key. Although it may subsequently be *used* to establish a C-HTTP connection, the public key does not explain anything

[4] In the "public key" section of the *Kiuchi* rejection, the Office points to an embodiment in the '504 patent specification in which SDNS 3313 answers a DNS query over an "administrative VPN or, alternatively, "in the clear." (*See* Second OA at 46-47, citing '504 patent 51:11-61.) It is unclear why the Office cites this embodiment, however, because it does not involve the return of a public key as the claimed "indication" or otherwise contravene the public key disclaimer in the '504 patent. (*See supra* Section II.C.) Thus, the cited embodiment does not support the Office's position that *Kiuchi*'s public key discloses the claimed indication.

about the capabilities of the C-HTTP name server. (Supp. Keromytis Decl. ¶ 38.) Indeed, *Kiuchi*'s public key is for communicating with the server-side proxy, and thus cannot not convey information about the security capabilities of the C-HTTP name server.[5] For at least this additional reason, the *Kiuchi* rejections should be withdrawn.

c. The Office's Position that the IP Address of the Server-Side Proxy in *Kiuchi* Discloses the Claimed "Indication" Is Unreasonable and Inconsistent with the Specification

As with the public key, the '504 patent also expressly identifies and disclaims the conventional DNS system characteristic of returning a requested IP address, and explains that the claimed DNS system configured to comprise an "indication" is directed at addressing drawbacks associated with such conventional DNS systems. (*See, e.g.*, Response at 52-53; *see supra* Section II.C.) In the face of this disclaimer, however, the Office maintains a similar unreasonable stance in connection with the return of a requested IP address.

In particular, the Office insists that *Kiuchi*'s C-HTTP name server returning the IP address of the server-side proxy discloses the claimed "indication." (Second OA at 48.) According to the Office, "the release of the IP address by the C-HTTP name server [of *Kiuchi*] cannot be viewed in isolation as a conventional domain name query for an IP address" because "the C-HTTP [name server] releases an error code and subsequently performs a conventional DNS lookup." (*Id.*, citing *Kiuchi* 65.) The Office relies on a passage of *Kiuchi* explaining that, "[i]f [the connection] is not permitted, [the C-HTTP name server] sends a status code which indicates an error. If a client-side proxy receives an error status, then it performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy." (*Kiuchi* 65.) Thus, the Office contends that the "ordinary" DNS lookup outside of C-HTTP is "conventional" while the lookup inside C-HTTP is "unconventional" in the context of the '504 patent. The Office's position is incorrect for at least two reasons.

First, *Kiuchi* has no bearing on how the '504 patent claims are interpreted, because claims are interpreted based on the *specification* during reexamination. *See* M.P.E.P. § 2258. Under the Office's rationale, because *Kiuchi* labels a DNS lookup outside of C-HTTP as "ordinary," the lookup of the IP address within C-HTTP must be "unconventional" and thus correspond to the claimed "indication." Aside from being illogical, the Office's reasoning is incorrect because it ignores the disclaimers in the '504 patent specification, which must be considered when interpreting the scope of claims under the Office's broadest reasonable interpretation standard (*id.*), and substitutes them with

[5] The Second Office Action does not address these arguments. For this additional reason, the Second Office Action should not have been made an ACP. *See* M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed."). Patent Owner therefore requests a new, nonfinal Office Action.

Kiuchi, which is irrelevant to the standard. Here, the '504 patent identifies and distinguishes the *return of an IP address*. Whatever might be "ordinary" or "unconventional" according to *Kiuchi* has no effect on this disclaimer. As a result, linking the claimed "indication" to the *return of an IP address* in *Kiuchi*, just as the Office has done, is improper. Indeed, just because the '504 patent specification or Patent Owner might refer to the disclaimed subject matter as "conventional" for convenience when explaining the scope of the claimed invention, this does not mean that whatever might be "unconventional" in *Kiuchi* automatically discloses the claimed "indication." *Kiuchi* has no impact on how to properly construe claim terms in the '504 patent—the specification does. The Office cannot construe the recited indication to cover configurations that the specification disparages and disclaims—the return of a public key and the return of an IP address.

Second, the Office misunderstands the disclosure of *Kiuchi*. *Kiuchi* does not teach that the *C-HTTP name server* (the alleged DNS system) requests the subsequent DNS lookup outside of C-HTTP. Instead, it is the *client-side proxy* that runs the lookup if it receives an "error status" from the C-HTTP name server: "If it is not permitted, [the C-HTTP name server] sends a status code which indicates an error. If a *client-side proxy* receives an error status, then *it* performs DNS lookup, behaving like an ordinary HTTP/1.0 proxy." (*Kiuchi* 65, emphases added; Supp. Keromytis Decl. ¶ 41.) To run this "conventional" DNS lookup, the client-side proxy would send a DNS request to a public DNS server outside of *Kiuchi*'s C-HTTP system, which would respond to the client-side proxy with the IP address corresponding to the domain name provided in the request, assuming it had the IP address. (Supp. Keromytis Decl. ¶ 41.) The C-HTTP name server—the alleged DNS system—has no role in this "conventional" DNS request. (*Id.*) Thus, to the extent that the Office is suggesting that the C-HTTP name server provides the claimed "indication" because it performs two lookups—one "ordinary" and one "unconventional"—the Office is incorrect.

d. The Nonce Value Does Not Disclose the Claimed Indication

The Office also highlights *Kiuchi*'s C-HTTP name server returning a nonce value as the claimed "indication." (Second OA at 45.) This is a new position never articulated in previous actions, and thus supports Patent Owner's position that the ACP status of the Second Office Action be withdrawn. Moreover, the Office does not support its position or explain how the nonce value conveys the security capabilities of the C-HTTP name server, which the Office points to as the claimed DNS system. (*See generally id.* at 45-47.) This is improper. A rejection based on obviousness "cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of

obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). For at least this reason, the rejection is not supported and should be withdrawn. Additionally, the nonce value disclosed by *Kiuchi* cannot be attributed to the claimed "indication" limitations for at least the following reasons.

First, as explained previously, the Office construes the claimed "indication" as "a visible message or signal to a user that the DNS system supports establishing a secure communication link," but never applies this construction to support the position that *Kiuchi*'s nonce value meets the claim limitations. (Second OA at 21-22.) Thus, the rejection is uninformative, does not demonstrate unpatentability, and should be withdrawn for the reasons discussed above in Section II.C.

Second, as discussed, even if the Office applied its "visible-message-or-signal" construction to *Kiuchi*'s nonce value, it would find that the nonce value does not meet the construction. *Kiuchi* does not teach that the system conveys the nonce value to a user in the form of "a visible signal or message." And even if it did, the user would have no idea what the random nonce codes meant. (Supp. Keromytis Decl. ¶ 38.) As a result, even if the nonce value were conveyed to the user as a "visible message or signal" (which it is not), the nonce value would not tell "[the] user that the DNS system supports establishing a secure communication link," as required by the Office's construction. Indeed, the nonce value contains no information about the security capabilities of the alleged DNS system.

Because *Kiuchi* does not disclose or suggest a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1, the rejection of the claims in view of *Kiuchi* are deficient and should be withdrawn.

e. *Kiuchi*'s C-HTTP Name Server Does Not Store Domain Names and Corresponding Network Addresses

Independent claim 1 also recites that the DNS system is configured to store "a plurality of domain names and corresponding network address." The Office contends that *Kiuchi* discloses this feature because "[a] client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL," and "the C-HTTP name server sends the IP address . . . of the server-side proxy." (OA at 18, incorporating Req. Ex. F-3 at 8, quoting *Kiuchi* 65.) Thus, according to the Office, the URL is the claimed "domain name" while the IP address of the server-side proxy is the claimed "network address."

But as Patent Owner's expert successfully explained at trial in the *VirnetX v. Apple* litigation, *Kiuchi*'s URL (the alleged domain name) does not correspond to the *server-side proxy* but to the *resource itself* located on an origin server. (*See* 11/05/2012 Trial Tr. Afternoon Sess. at 39:3-41:20,

attached as Exhibit A-11.) For example, *Kiuchi* explains that the URL "http://server.in.current.connection!sample.html=@=6zdDfldfcZLj8V!i" represents a "resource name," and that when the URL is clicked, "the client-side proxy takes of the connection ID and forwards, the stripped, original *resource name* to the *server* . . . ." (*Kiuchi* 65, emphasis added.) As a result, the URL (the alleged domain name) does not correspond to the IP address of the *server-side proxy* (the alleged corresponding network address) but to a *resource on the origin server.* And when the C-HTTP name server is provided with the URL of a resource, it responds not with the resource's corresponding network address but with the IP address of the server-side proxy. Accordingly, the C HTTP name server in *Kiuchi* is not configured to "store a plurality of domain names and corresponding network addresses," as recited in claim 1.

Appendix 2.1 of *Kiuchi* describes the format of a "C-HTTP name service request." (*Kiuchi* 72.) As shown, the name service request includes a field "SERVER-SIDE-PROXY-NAME." (*Id.*) As Patent Owner's expert successfully explained at trial, one of ordinary skill in the art would have recognized that the "SERVER-SIDE-PROXY-NAME" field actually refers to the URL of the *resource* on the origin server being requested, and not to the domain name of the *server-side proxy*. (Ex. A-11 at 39:20-40:11.) In fact, the author, Dr. Kiuchi, confirmed that this is the case in a 1996 slide presentation on C-HTTP accompanying his paper that he gave to the Institute of Electrical and Electronics Engineers ("IEEE"). (*See generally Kiuchi* Slide Presentation, attached as Exhibit A-12.) For example, slide 9 explains that the C-HTTP name server "keeps" "resource names." (*Id.* at 9). Additionally, slide 17 illustrates that a C-HTTP name request includes a "RESOURCE-NAME," (*id.* at 17), while slide 20 shows that the C-HTTP name response that follows includes a "SERVER-SIDE-PROXY-IP [address]," (*id.* at 20). Indeed, *Kiuchi*'s system would not work if the client-side proxy requested a domain name for the server-side proxy from the C-HTTP name server instead of a name for a resource on the origin server. (*See* Ex. A-11 at 40:15-20, "Q. Would the *Kiuchi* system work if the client-side proxy requested a domain name for the server-side proxy from C-HTTP? A. No. The way *Kiuchi* has to work is that what's being requested is the resource that's on the origin server. That's where the data is.")

Accordingly, contrary to the Office's positions, *Kiuchi* does not disclose the C-HTTP name server storing domain names and corresponding network addresses.

f. *Pfaffenberger* Does Not Remedy the Deficiencies of *Kiuchi*

In its Response, Patent Owner explained that *Pfaffenberger* fails to remedy the deficiencies of *Kiuchi*. (*See* Response at 53-55.) The Office did not respond to Patent Owner's arguments, except to state that "*Kiuchi* is not deficient in the manner asserted by the patent owner." (Second OA

at 48.) The Office thus does not challenge Patent Owner's position that *Pfaffenberger* does not disclose or suggest the claimed features that are missing from *Kiuchi.* Moreover, *Pfaffenberger* fails to disclose any DNS system, much less one configured to store domain names and corresponding network addresses. Accordingly, for the reasons above and the explained in the Response, *Pfaffenberger* does not remedy the deficiencies of *Kiuchi*, and the combination of the two references fails to disclose or suggest the claimed DNS system. (Response at 53-55.) The rejections in light of these references should be withdrawn.

g. One of Ordinary Skill in the Art Would Not Have Relied on *Pfaffenberger*

In addition, as explained in the Response, *Pfaffenberger* is nonanalogous art because it is not reasonably pertinent to the problem solved by the claims, namely, enabling secure communications easily and conveniently. (Response at 55.) The Office finds this argument "unpersuasive" because enabling secure communications easily and conveniently "is not claimed, and thus the patent owner's arguments are essentially directed to unclaimed features." (Second OA at 49.) Patent Owner respectfully submits that the Office's basis for circumventing Patent Owner's argument is improper, and that the rejection should be withdrawn, for the reasons discussed above in Section IV.C.

For the above-noted additional reasons, the rejection of independent claim 1 based on *Kiuchi* and *Pfaffenberger* should be withdrawn, and the claim should be confirmed.

2. Independent Claims 36 and 60

Independent claims 36 and 60 include recitations similar to those discussed above in connection with claim 1. Additionally, the Office rejected claims 36 and 60 for the same reasons it rejected claim 1. Thus, for reasons similar to those described above and in the Response with respect to claim 1, *Kiuchi-Pfaffenberger* does not render obvious claims 36 and 60, and the rejections should be withdrawn.

3. Dependent Claims 8 and 9

Claims 8 and 9 depend from independent claim 1 and includes all of its features. Thus, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claims 8 and 9, and the rejection of these claims should be withdrawn, at least for the reasons discussed above in connection with independent claim 1. Claim 8 also distinguishes over the cited art for additional reasons. For example, claim 8 recites that "the domain name service system is connectable to a virtual private network through the communication network." Claim 9 incorporates these features because it depends from claim 8. The combination of *Kiuchi* and *Pfaffenberger* does not disclose or suggest these additional features.

In its Response, Patent Owner provided several reasons why the *Kiuchi-Pfaffenberger* combination fails to render obvious claims 8-10, 12, and 13. (*See* Response at 56-59.) One of those reasons is that *Kiuchi* fails to disclose or suggest the claimed "virtual private network," as one of ordinary skill in the art would have understood that term in the context of the '504 patent. (*See id.*) The Office finds that argument unpersuasive, instead offering its own definition of "virtual private network." (Second OA at 49-50.) Patent Owner submits that its interpretation of the claimed "virtual private network" is correct for the reasons discussed in the Response, and that the rejection of claims 8 and 9 should therefore be withdrawn and the claims confirmed as patentable.

Patent Owner also raised an additional argument with respect to claims 8 and 9, an argument which the Office does not address in the Second Office Action. (*Compare* Response at 58-59 *with* Second OA at 49-51.) In particular, *Kiuchi* does not teach that the alleged domain name service system (the *C-HTTP name server*) is connectable to the alleged virtual private network (the C-HTTP connection between the *client-side proxy* and *server-side proxy*), as recited in these claims. (Response at 58-59.) For this additional reason, the rejection of claims 8 and 9 is improper and should be withdrawn. Moreover, since the Office did not fully address the Response, the Second Office Action should not have been designated an ACP. *See* M.P.E.P. § 2671.02 ("Before an ACP is in order, a clear issue should be developed."). Should the Office maintain its rejection of claims 8 and 9, Patent Owner requests that the next action be a nonfinal Office Action.

4. Dependent Claims 24 and 48

Dependent claims 24 and 48 depend from independent claims 1 and 36, respectively, and thus include all of the features of these claims. Accordingly, the combination of *Kiuchi* and *Pfaffenberger* does not render obvious claims 24 and 48, and the rejection of these claims should be withdrawn, at least for the reasons discussed above in connection with independent claims 1 and 36, and those discussed in the Response. (Response at 63-64.) Claims 24 and 48 distinguish over the combination for additional reasons as well.

For example, claim 24 recites that "at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link," and claim 48 similarly recites that "at least one of the plurality of domain names includes an indication that the domain name service system supports the establishment of a secure communication link." The Office presents two reasons why, in its view, "the domain name 'another.server.in.closed.network'" in *Kiuchi* discloses the claimed "indication." (Second OA at 51-52.) First, according to the Office, "the domain name 'another.server.in.closed.network' provides an indication that the *host (server)* corresponding to the name (closed) is secure at least to the extent

that it is 'closed'." (*Id.* at 52, emphasis added.) The Office's reasoning is inconsistent with the claim language. Even if the Office were correct that "the domain name 'another.server.in.closed.network' indicates that the *host (server)* corresponding to the domain name is secure" (emphasis added), *the host is behind the server-side proxy firewall and separate from the C-HTTP name server*, which the Office points to as the claimed domain name service system. (*See, e.g.*, *Kiuchi* 66, "It is possible to map any of the virtual directories on the server-side proxy to any of the directories in *one or more origin servers inside the firewall*," emphasis added, and "a server-side proxy communicates with *an origin server inside the firewall*," emphasis added.) Conveying information about a "host (server)" behind the server-side proxy firewall in *Kiuchi* indicates nothing about the capabilities of the C-HTTP name server, the alleged DNS system, to support establishing a secure communication link.

The Office's other position with respect to claims 24 and 48 is that "the domain name 'another.server.in.closed.network' . . . also indicates that a DNS system will resolve the domain name into an IP address and public key to support the establishment of a connection to the secure (closed) server." (Second OA at 52.) Thus, according to the Office, an indication that a DNS system *will* resolve the alleged domain name is an indication that the DNS system supports establishing a secure communication link, as claimed. However, even if the Office's view is correct (which Patent Owner does not concede), by the time *Kiuchi*'s alleged domain name is displayed, the C-HTTP name server has *already* resolved it into an address. (Supp. Keromytis Decl. ¶ 42.) *Kiuchi* states that "[w]hen one of these resource names with a connection ID, for example, 'http://server.in.current.connection!sample.html=@=6zd DfldfcZLj8V!i' in Figure (b), is selected and requested by an end-user, the client-side proxy takes off the connection ID and *forwards the stripped, the original resource name to the server* in its request as described in Figure (c)." (*Kiuchi* 65, emphasis added.) Since the client-side proxy immediately strips and forwards the original resource name to the server upon the URL being clicked without first needing to resolve the address of the server, *the address has already been resolved*. (Supp. Keromytis Decl. ¶ 42.) Thus, contrary to the Office's allegation, the alleged domain name another.server.in.closed.network is not an indication that a DNS system *will* resolve the domain name. Accordingly, the URL "another.server.in.closed.network" does not disclose the claimed "indication" as alleged by the Office.

Finally, the Office attempts to sidestep claims 24 and 48 on the ground that they allegedly define "nonfunctional descriptive material" that is not afforded patentable weight. (*See* Second OA at 52.) The Office is incorrect for the reasons discussed above in Section III.A.5.