Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

VIRNETX, INC. AND SCIENCE APPLICATION INTERNATIONAL CORPORATION,
Patent Owner

Patent No. 8,051,181
Issued: November 1, 2011
Filed: February 27, 2007
Inventors: Victor Larson, *et al.*
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Inter Partes Review No. IPR2014-00486

PETITION FOR INTER PARTES REVIEW

TABLE OF CONTENTS

I. COMPLIANCE WITH REQUIREMENTS FOR A PETITION FOR INTER PARTES REVIEW

A. Certification the '181 Patent May Be Contested by Petitioner

Petitioner certifies that U.S. Patent No. 8,051,181 (the '181 patent) (Ex. 1025) is available for *inter partes* review. Neither Petitioner, nor any party in privity with Petitioner, has filed a civil action challenging the validity of any claim of the '181 patent. The '181 patent also has not been the subject of a prior *inter partes* review by Petitioner or a privy of Petitioner.

The '181 patent was asserted against Petitioner in proceedings alleging infringement as explained in § C.2, below. This petition is nonetheless proper as it is accompanied by a motion for joinder to (i) IPR2014-00483 and -00484 filed by Apple, and (ii) IPR2014-00403 and -00404 filed by Microsoft. The one-year period specified in § 315(b) does not apply to a petition that is accompanied by a request for joinder under 35 U.S.C. § 315(c). For the reasons in § III.B below and in the accompanying motion for joinder, proceedings based on the petitions should be joined to enable review of these admittedly patentably indistinct patent claims.

B. Fee for Inter Partes Review (§ 42.15(a))

The Director is authorized to charge the fee specified by 37 CFR § 42.15(a) to Deposit Account No. 50-1597.

C. Mandatory Notices (37 CFR § 42.8(b))

1. Real Party in Interest (§ 42.8(b)(1))

The real party of interest of this petition pursuant to § 42.8(b)(1) is Apple Inc. ("Apple") located at One Infinite Loop, Cupertino, CA 95014.

2. Other Proceedings (§ 42.8(b)(2))

On November 1, 2011, Petitioner was served with a complaint for infringement of the '181 patent, which resulted in civil action no. 11-cv-00563-LED (E.D. TX). This action was stayed after Patent Owner, on November 4, 2011, filed a complaint in the International Trade Commission, which resulted in investigation no. 0337-TA-818. That investigation was withdrawn on July 20, 2012. On September 28, 2012, Patent Owner filed another complaint in the ITC, resulting in investigation no. 337-TA-858, which also was withdrawn (on May 15, 2013). In June 2013, the stay in the Texas litigation was lifted and the action consolidated with civil action no. 6:12-cv-00855-LED. Patent Owner did allege infringement of the '181 patent in the latter action.

The '181 patent also is the subject of *inter partes* reexamination Control No. 95/001,949 where all claims stand finally rejected. The Office issued a Right of Appeal Notice in the '949 proceeding on August 16, 2013.

3. Designation of Lead and Backup Counsel

Lead Counsel	Backup Lead Counsel
Jeffrey P. Kushan (Reg. No. 43,401) **jkushan@sidley.com** (202) 736-8914	Joseph A. Micallef (Reg. No. 39,772) **jmicallef@sidley.com** (202) 736-8492

4. Service Information (§ 42.8(b)(4))

Service on Petitioner may be made by e-mail, or by mail or hand delivery to: Sidley Austin LLP, 1501 K Street, N.W., Washington, D.C. 20005. The fax number for lead and backup counsel is (202) 736-8711.

D. Proof of Service (§§ 42.6(e) and 42.105(a))

Proof of service of this petition is provided in **Attachment A**.

II. Identification of Claims Being Challenged (§ 42.104(b))

Claims 1-29 of the '181 patent are unpatentable as being anticipated under 35 U.S.C. § 102(a), (b) & (e), and/or for being obvious over the prior art under 35 U.S.C. § 103. Specifically:

(i) Claims **1-29** are anticipated under § 102(e) by U.S. Patent No. 6,496,867 to Beser ("Beser") (Ex. 1031);

(ii) Claims **1-29** are obvious under § 103 based on Beser (Ex. 1031) in view of RFC 2401 (Ex. 1032);

(iii) Claims **3-4** and **23** are obvious under § 103 based on Beser (Ex. 1031) in view of Kiuchi (Ex. 1004);

(iv) Claims **22** and **24-27** are obvious under § 103 based on Beser (Ex. 1031) in view of RFC 2543 (Ex. 1032);

(v) Claims **1-6, 8-9, 13-19** and **21-29** are anticipated under § 102(b) by Kiuchi (Ex. 1004).

Petitioner's proposed construction of the claims, the evidence relied upon, and the precise reasons why the claims are unpatentable are provided in § **IV**, below. The evidence relied upon in support of this petition is listed in **Attachment B**.

III. Relevant Information Concerning the Contested Patent

A. Effective Filing Date and Prosecution History of the '181 patent

The ’181 patent issued from U.S. Application No. 11/679,416, filed February 27, 2007, which is a continuation of U.S. Application No. 10/702,486 (issued as U.S. Patent No. 7,188,180) (the ’180 patent). Ex. 1025 at 81. The ’486 application is a division of U.S. Application No. 09/558,209, filed April 26, 2000, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000 (issued as U.S. Patent No. 6,502,135) (the ’135 patent). The ’783 application is a continuation-in-part of U.S. Application No. 09/429,643, filed on October 29, 1999, and claims priority to Provisional Application Nos. 60/106,261, filed October 30, 1998 and 60/137,704, filed June 7, 1998.

Claims 1, 2, 24, 26, 28, and 29 are independent claims. Each of these claims relies on information found only in the disclosures of applications filed on or after April 26, 2000, the date the ’209 application was filed. For example, each independent claim recites a “**secure name**” or a “**secure name service**.” There is no mention of the terms “**secure name**” and “**secure name service**” in any application filed prior to the ’209 application, much less a sufficient written description of these terms as they are used in the claims of the ’181 patent. In fact, even the ’209 and subsequently filed applications themselves provide no written description support for these claim elements and concepts. Instead, they describe a

"**secure domain name service**."0F[1] Accordingly, the effective filing date for claims 1-29 of the '181 patent cannot be earlier than the filing date of the'209 application, April 26, 2000. This also is consistent with Patent Owner's position during the *inter partes* reexamination of the '180 patent, where it acknowledged the priority date of the '180 patent was not earlier than April 26, 2000. Ex. 1023 at 232.

B. Relationship to U.S. Patent Nos. 7,987,274 and 7,188,180

Patent Owner has admitted the claims of the '181 patent are not patentably distinct from claims in the '180 patent (parent of the '181 patent) and U.S. Patent No. 7,987,274 (the '274 patent) (child of the '181 patent). During prosecution of the '181 patent, the Office imposed obviousness-type double patenting rejections of the pending claims over (i) claim 1 of co-pending application 11/839,987, which issued as the '274 patent, and (ii) claim 1 of the '180 patent. Ex. 1026 at 815. Patent Owner did not dispute these findings, but instead filed terminal disclaimers to obviate the rejections. Ex. 1026 at 795-797, 815, 1045 (10/8 & 11/4/2010). Similarly, the Office rejected claims that issued in the '274 patent for obviousness-

[1] During prosecution of the '181 patent, Patent Owners contended a "secure name" and "Secure name service" was a subset of a "**secure name service**." Ex. 1029 at ¶¶ 224-226; *see* Ex. 1026 at 813 (Remarks Oct. 8, 2010).

type double patenting over claims in each of the ’180 and ’181 patents. Ex. 1028 at 183-186, 250, 380-381. Again, Patent Owner did not dispute these findings, but instead filed terminal disclaimers over the ’180 and ’181 patents to obviate the double patenting rejections. *See* Ex. 1028 at 2741 and 296; *see id.* at 632 and 282. By acquiescing to, rather than contesting, the findings of obviousness-type double patenting, Patent Owner has conceded the ’180, ’181 and ’274 claims are not patentably distinct. A final written decision finding the subject matter of claims in either of the ’274 or the ’180 patents unpatentable would estop Patent Owner from contending the claims in the ’181 are patentable. *See* 37 C.F.R. 42.73(d)(3). Among other things, such a finding would preclude Patent Owner from asserting the ’181 patent claims are patentable in the currently pending *inter partes* reexamination proceeding (*i.e.*, Reexamination Control No. 95/001,949).

C. Person of Ordinary Skill in the Art

A person of ordinary skill in the art in the field of the ’181 patent would have been someone with a good working knowledge of networking protocols, including those employing security techniques, as well as computer systems that support these protocols and techniques. The person also would be very familiar with Internet standards related to communications and security, and with a variety of client-server systems and technologies. The person would have gained this

knowledge either through education and training, several years of practical working experience, or through a combination of these. Ex. 1029 ¶ 59.

D. Construction of Terms Used in the Claims

In this proceeding, claims must be given their broadest reasonable interpretation in light of the specification. 37 CFR § 42.100(b). In reaching its conclusions about the meaning of the claims, the Board should consider Patent Owner's contentions in concurrent litigation involving the '181 and closely related patents including the '697, '135, '151, '504 and '211 patents. Also, if Patent Owner contends terms in the claims have a special meaning, those contentions should be disregarded unless Patent Owner also amends the claims compliant with 35 U.S.C. § 112 to make them expressly correspond to those contentions. *See* 77 Fed. Reg. 48764 at II.B.6 (August 14, 2012); *cf. In re Youman*, 679 F.3d 1335, 1343 (Fed. Cir. 2012). In the constructions below, Petitioner identifies representative subject matter within the scope of the claims read with their broadest reasonable interpretation. Petitioner expressly reserves its right to advance different constructions in district court litigation, which employs a different claim construction standard.

1. Secure Name

The '181 patent disclosure does not use, much less define, the term "**secure name.**" In the claims, a "**secure name**" is said to be associated with a network

address of a first or second device. *See, e.g.*, claim 2 ("…the message requesting a network address associated with the secure name of the second device"). The claims also differentiate a "**secure name**" from an "**unsecured name**." *See, e.g.*, claims 21, 26. The portrayal of a "secure name" in this manner is consistent with arguments Patent Owner made during prosecution. *See, e.g.*, Ex. 1026 ('181 FH) at 813 ("… Applicant submits that a "secure name" is a name associated with a network address associated of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device.").

Patent Owner also contended during prosecution that a "**secure name**" is broader in its meaning than a "**secure domain name**." As it stated:

> The claimed "secure name" includes, but is not limited to, a secure domain name. For example, a "secure name" can be a secure non-standard domain name, such as a secure non-standard top-level domain name (*e.g.*, .scom) or a telephone number.

Ex. 1026 (181 FH) at 813; Ex. 1029 at ¶¶ 212-214.

Patent Owner discussed the meaning of the term "**secure domain name**" in two reexaminations of the '180 patent. In Control No. 95/001,270, Patent Owner argued that the claim terms "**secure domain name**" and "**secure domain name service**" had meanings different than the conventional meaning of the terms

"**domain name**" and "**domain name service**." Specifically, Patent Owner contended "a secure domain name is a [sic] 'a non-standard domain name.'" Ex. 1023 at 229-31. Patent Owner also explained that a "**secure domain name**" was different from a standard domain name because a secure domain name cannot be resolved using a conventional domain name server. *See* Ex. 1029 at ¶¶ 210-235. The Office adopted Patent Owner's contentions in the ACP, stating:

> The '180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a convention[al] domain name server using a secure domain name will result in a return message indicating that the URL is unknown ('180 patent at 51:25-35) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name ('180 patent at 51:25-35). (emphasis added)

Ex. 1023 (95/001,270 FH) at 129-130 (ACP (Jun. 16, 2010)).

In view of these considerations, the broadest reasonable interpretation of the term "secure name" would encompass a "*non-standard domain name that cannot be resolved by a conventional domain name server*." Ex. 1029 at ¶¶ 209-215. Included within this definition would be non-standard domain names such as telephone numbers or non-standard top-level domains.

2. Secure Domain Name

The ’181 patent does not define the term “**secure domain name**.” As explained in § 1 above, Patent Owner represented during prosecution of the ‘181 patent that a “**secure name**” is not a conventional domain name and cannot be resolved using a conventional domain name server. The term “secure domain name,” because it uses an additional term, is arguably narrower than a “**secure name**” by the use of a “domain name” rather than simply a “name.” A “domain name” would be understood by a person of ordinary skill to be a hierarchical sequence of words in decreasing order of specificity that corresponds to a numerical IP address. Ex. 1029 at ¶¶ 85-87; *see generally* ¶¶ 82-90. Patent Owner has contended, however, the term “domain name” is simply “a name corresponding to an IP address” (*see, e.g.*, Ex. 1066 at 14-15). Considering these points, the term “**secure domain name**” in its broadest reasonable interpretation would encompass a “*non-standard domain name that corresponds to a network address and cannot be resolved by a conventional domain name server*.” *See* Ex. 1029 at ¶¶ 209-242.

3. Unsecured Name

The ’181 patent does not expressly define the term “**unsecured name**.” In contrast to a “secure name”, a person of ordinary skill would understand that an “unsecured name” would include a conventional domain name that can be resolved by a conventional domain name server. The use of “name” rather than “domain name,” however, indicates the term in its broadest reasonable interpretation is

broader than simply a "domain name," and would include any name that identifies a computer. Ex. 1029 at ¶¶ 247-250. This interpretation is consistent with Patent Owner's contentions in litigation, where it asserted an "unsecured name" is "*a name that can be resolved by a conventional name service*." Ex. 1071 at 2. Thus, the term "unsecured name" in its broadest reasonable interpretation at least encompasses "*a name that can be resolved by a conventional name service.*"

4. Secure Name Service

There is no mention of the term "**secure name service**" in the '181 patent disclosure. Instead, this phrase appears only in the claims, and was first added by an amendment to the claims during examination. Ex. 1026 at 806 (Claims Oct. 8, 2010). In connection with that amendment, Patent Owner argued a "secure name service is a service for resolving secure names into network addresses." Ex. 1026 at 812 (Remarks Oct. 8, 2010) (emphasis in original). Based on Patent Owner's contentions, a "secure name service" in its broadest reasonable interpretation would include any type of name service that can act on secure names (*e.g.*, by providing the network address corresponding to the secure name), including a "**secure domain name service**" specified in the '180 patent claims. Ex. 1029 at ¶¶ 224-226, 233-234. The broadest reasonable interpretation of a "*secure name service*" thus would include "*a service that can resolve network addresses for a*

secure name for which a conventional name service cannot resolve addresses." Ex. 1029 at ¶ 235; *see id.* at ¶¶ 216-234.

5. Secure Communication Link

The '181 patent explains a "secure communication link" is "a virtual private communication link over the computer network." Ex. 1025 at 6:57-59. A "secure communication link" therefore encompasses a VPN. Ex. 1029 at ¶¶ 252-256. In its broadest reasonable interpretation, a "secure communication link" (like a VPN) enables computers to privately and directly communicate with each other over a public network. *See, e.g.*, Ex. 1025 at 39:4-13. A person of ordinary skill would have understood in April of 2000 that any technique that protects the anonymity of the computers involved in the communications could be used to establish a VPN. Such a person would have understood that a VPN could be established without encrypting the network traffic (*e.g.*, by using "obfuscation" techniques to ensure the security and anonymity of the network traffic over a public network). *See* Ex. 1029 ¶¶ 258-260; *id.* at ¶¶ 124-126, 137-140; Ex. 1043 at 2; Ex. 1044 at 2-4. This is consistent with '181 patent disclosure. *See, e.g.*, Ex. 1025 at 1:50-51 ("Data security is <u>usually</u> tackled using some form of data encryption"); 2:37-47 (referring to technique that does not use encryption to protect the anonymity of the VPN); *see also* Ex. 1029 ¶¶ 258-260. The '181 patent also shows use of TARP routers that do encrypt all network traffic (Ex. 1025 at 3:6-3:36), but does not state that TARP

routers are required for the disclosed DNS-based VPN scheme. *See, e.g.*, Ex. 1025 at 39:32-36 ("The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above…" (emphasis added)). The '181 patent also does not show any encryption steps in the DNS-related VPN schemes it describes. *See* Ex. 1025 at 38:51-41:40.

Patent Owner also has contended in other proceedings involving related patents that a "secure communication link" (e.g., a VPN) encompasses direct communications between computers transmitted via intermediary computers and devices. One district court has found, for example, that the common disclosure in the '181 and '135 patents suggests that the "…routers, firewalls, and similar servers that participate in typical network communication do not impede 'direct' communication between a client and target computer." Ex. 1018 at 8 (FN2).

In view of these considerations, the broadest reasonable interpretation of "*secure communication link*" would encompass "*a communication link in which computers privately and directly communicate with each other on insecure paths between the computers where the communication is both secure and anonymous, and where the data transferred may or may not be encrypted*." *See* Ex. 1029 at ¶¶ 251-260.

IV. Precise Reasons for Relief Requested

A. Claims 1-29 Are Anticipated by Beser

Beser has an effective filing date of August 27, 1999, and is prior art under at least under §102(e). Ex. 1031 at 1. Petitioner submits that claims 1-29 of the '181 patent are unpatentable in view of Ex. 1031 (Beser), considered alone or in conjunction Ex. 1032 (RFC 2401) and knowledge in the field of the '181 patent, for the reasons set forth below, as supported by ¶¶ 277-371 of Ex. 1029.

1. Beser Anticipates Claims 1 and 29

Beser (Ex. 1031) describes systems that establish an IP tunneling association between two end devices with the aid of a first and second network device and a trusted-third-party network device on a public network. Ex. 1029 at ¶¶ 277-286. Beser shows that the originating end device is associated with the first network device and the terminating end device is associated with the second network device. Ex. 1029 at ¶¶ 282-283, 285, 302-305; *see id.* at ¶¶ 329-339. Beser explains that the first and second network devices may be edge routers, "gateway" computers, or other network devices. Ex. 1029 at ¶¶ 282-283, 286, 302-305, 316-317, 337-339. Beser explains the trusted-third-party network device can be a domain name server, and it also can include a subscriber phone number directory service. Ex. 1029 at ¶¶ 284-287, 305-309; *see id.* at ¶¶ 282, 324-331.

Beser explains the originating and terminating devices can be VOIP devices such as phones or personal computers. Ex. 1029 at ¶¶ 279, 282-283, 294-299; *see id.* at ¶¶ 286-287. Beser shows each end device is associated with multiple

identifiers, including a unique identifier that is registered with the trusted-third-party network device and is used to initiate secure IP tunnels. Ex. 1029 at ¶¶ 318-323. Beser describes a configuration where each end device is associated with a phone number, a domain name, and a public IP address. Ex. 1029 at ¶¶ 290-291, 322-323; *see id.* at ¶¶ 306, 336, 339. Beser shows that, in that configuration, the phone number can be the unique identifier registered with the trusted-third-party network device, (Ex. 1029 at ¶¶ 306-309, 319-323), while the domain name is a standard domain name registered with a standard name server. Ex. 1029 at ¶¶ 322-323, 379-380, 551. Therefore the terminating end device has a secure name (*e.g.*, the phone number that is registered with the trusted-third-party network device) and an unsecured name (*e.g.*, its domain name). *See* §§ III.D.1-III.D.3.

The Beser systems are implemented using programmed computers and other programmable devices that have storage media containing code that configures how those devices function. Ex. 1029 at ¶ 382. Beser thus shows "*A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name*" as specified in **claim 1**. Ex. 1029 at ¶¶ 372-383. Beser also shows "*A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name*," as specified in **claim 29**. Ex. 1029 at ¶¶ 615-623.

To establish an IP tunnel, the originating end device sends a request containing a unique identifier (*e.g.*, a phone number) specifying a destination (*i.e.*, a terminating end device). Ex. 1029 at ¶¶ 285, 314-324. The first network device receives the request, evaluates it, and then sends it to the trusted-third-party network device, if appropriate. Ex. 1029 at ¶¶ 316-317; *see id.* at ¶¶ 302-305. Beser explains that after the trusted-third-party network device receives the request, it evaluates the request to determine whether it contains a unique identifier that is associated with a secure terminating device. Ex. 1029 at ¶¶ 324-331. For example, if the identifier (*e.g.*, a phone number) is listed in the trusted-third-party network device's directory of subscribers, the identifier corresponds to a secure destination. Ex. 1029 at ¶¶ 284-286, 305-309, 324-331. The trusted-third-party network device's directory of subscribers associates each subscriber's phone number to the IP addresses of that subscriber's end device and second network device. Ex. 1029 at ¶¶ 284-287, 324-329. Thus, the IP address of the second network device is associated with the terminating end device. Ex. 1029 at ¶ 388.

If the unique identifier corresponds to a secure destination, the trusted-third-party network device will automatically initiate an IP tunnel between the end devices by negotiating private IP addresses that will be used to transmit data between these end devices across a public network. Ex. 1029 at ¶¶ 278-281, 326-338. First, the trusted-third-party network device will send a message to the

second network device requesting to negotiate private IP addresses. Ex. 1029 at ¶¶ 329-331. Then, the private IP address for the originating device will be transmitted from the first network device to the second network device through the trusted-third-party network device. Ex. 1029 at ¶¶ 329-331. Each of the messages sent to the second network device is a message indicating the originating device desires to communicate securely with the terminating device. Ex. 1029 at ¶¶ 387-390. To complete the exchange of private IP addresses, the private IP address for the terminating device is transmitted from the second network device to the first network device via the trusted-third-party network device. Ex. 1029 at ¶¶ 332-335. Beser shows these messages can be encrypted. Ex. 1029 at ¶¶ 340-342. Beser thus shows "*receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device*" as specified in **claim 1**. Ex. 1029 at ¶¶ 384-391. Beser also shows "*receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered*" as specified by **claim 29**. Ex. 1029 at ¶¶ 624-631.

After the private network addresses are negotiated, the first network device will inform the originating device of the private IP address associated with the terminating device. Ex. 1029 at ¶¶ 330-334. The originating device can then

securely transmit data to the terminating device by sending IP packets to the private IP address. Ex. 1029 at ¶¶ 336-339, 289-290. Similarly, the terminating device can then securely transmit data to the originating device by sending IP packets to the private IP address. *Id.* Beser explains that IP traffic within an IP tunnel ordinarily will be encrypted utilizing the techniques described in RFC 2401 (*i.e.*, under the IPsec protocol), and that encryption of the tunneling connection occurs automatically. Ex. 1029 at ¶¶ 291-293, 325, 342-353. The IP tunnels described in Beser permit end devices to directly communicate over a secure and anonymous channel. Ex. 1029 at ¶¶ 278-281, 289-293, 336-339. Beser thus shows a method comprising the step of "*sending a message over a secure communication link from the first device to the second device*" as specified in **claim 1**. Ex. 1029 at ¶¶ 392-395. Beser thus shows "*sending a message securely from the first device to the second device*" as specified by **claim 29**. Ex. 1029 at ¶¶ 632-636. Therefore, Beser anticipates **claims 1** and **29**.

2. Beser Anticipates Claims 2 and 28

As explained in § 1, Beser discloses methods for establishing a secure IP tunneling association between an originating end device and a terminating end device. Thus, for the same reasons, Beser shows a "*method of using a first device to communicate with a second device having a secure name*" as specified in **claim 2**. Ex. 1029 at ¶¶ 402-409. Beser also shows "*A non-transitory machine-readable*

medium comprising instructions," specified in **claim 28**. Ex. 1029 at ¶¶ 586-593.

To establish an IP tunnel, Beser shows the originating end device sends a request containing a unique identifier (*e.g.*, a phone number) specifying a destination (*i.e.*, a terminating end device). Ex. 1029 at ¶¶ 285, 314-324. The first network device receives the request, evaluates it, and then sends it to the trusted-third-party network device, if appropriate. Ex. 1029 at ¶¶ 316-317; *see id.* at ¶¶ 302-305. Beser explains that after the trusted-third-party network device receives the request, it evaluates the request to determine whether it contains a unique identifier that is associated with a secure terminating device. Ex. 1029 at ¶¶ 324-331. For example, if the identifier (*e.g.*, a phone number) is listed in the trusted-third-party network device's directory of subscribers, the identifier corresponds to a secure destination. Ex. 1029 at ¶¶ 284-287, 305-309, 324-331. The trusted-third-party network device's directory of subscribers associates each subscriber's phone number to the IP addresses of the subscriber's network device and of the subscriber's end device. Ex. 1029 at ¶¶ 284-285. Thus, Beser shows the trusted-third-party network device can resolve dial-up phone numbers into IP addresses. Ex. 1029 at ¶¶ 284-287, 324-331. Beser shows that the trusted-third-party network device can require "encryption or authentication." Ex. 1029 at ¶¶ 291-293, 325, 340-353. The trusted-third-party network device is a secure name server. Ex. 1029 at ¶¶ 324-329, 414-415, 599-600.

Beser thus shows "*from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device*," as specified in **claim 2**. Ex. 1029 at ¶¶ 410-417. Beser also shows "*sending a message to a secure name service, the message requesting a network address associated with a secure name of a device*" as specified by **claim 28**. Ex. 1029 at ¶¶ 595-602.

Beser shows that if the unique identifier corresponds to a secure destination, the trusted-third-party network device will automatically negotiate an IP tunnel between the end devices by negotiating private IP addresses that will be used to transmit data between these end devices across a public network. Ex. 1029 at ¶¶ 278-281, 326-338. The trusted-third-party network device will send a message to the second network device requesting to negotiate private IP addresses. Ex. 1029 at ¶¶ 329-331. The second network device is associated with the terminating end device. Ex. 1029 at ¶¶ 282-283, 285, 302-305. The trusted-third-party network device also will inform the first network of the second network device's IP address. Ex. 1029 at ¶¶ 330-337. Therefore, the first network device receives a message containing a network address associated with the secure name of the terminating device. Ex. 1029 at ¶¶ 419, 604.

Then, the private IP address for the originating device will be transmitted from the first network device to the second network device through the trusted-

third-party network device. Ex. 1029 at ¶¶ 329-331. The private IP address for the terminating device will be transmitted from the second network device to the first network device through the trusted-third-party network device. Ex. 1029 at ¶¶ 332-335. Therefore, the first network device receives a message containing a network address associated with the secure name of the terminating device. Ex. 1029 at ¶¶ 421, 606. Beser shows these messages can be encrypted. Ex. 1029 at ¶¶ 340-342. After the private addresses are negotiated, the first network device will inform the originating device of the private IP address associated with the terminating device. Ex. 1029 at ¶¶ 330-331, 334. Therefore, it receives a message containing a network address associated with the secure name of the terminating device. Ex. 1029 at ¶¶ 422, 607. Beser thus shows "*at the first device, receiving a message containing the network address associated with the secure name of the second device,*" as specified in **claim 2**. Ex. 1029 at ¶¶ 418-423. Beser thus shows "*receiving a message containing the network address associated with the secure name of the device*" as specified by **claim 28**. Ex. 1029 at ¶¶ 603-608.

Beser shows that the trusted-third-party network device can require "encryption or authentication" of any communications exchanged with it. Ex. 1029 at ¶¶ 291-293, 325, 340-353. Therefore, during the negotiation process, the first network device sends a message to the address associated with the terminating device using a secure communication link. Ex. 1029 at ¶¶ 424, 609. The

originating device can then securely transmit data to the terminating device by sending IP packets to the private IP address. Ex. 1029 at ¶¶ 289-290, 336-339. The originating network device thus sends a message to the address associated with the terminating device using a secure communication link. Ex. 1029 at ¶¶ 425, 610. Similarly, the terminating device can securely transmit data to the originating device by sending IP packets to the private IP address. Ex. 1029 at ¶¶ 336-339. Beser explains that IP traffic within an IP tunnel ordinarily will be encrypted utilizing the techniques described in RFC 2401 (*i.e.*, under the IPsec protocol), and that encryption of the tunneling connection occurs automatically. Ex. 1029 at ¶¶ 291-293, 325, 342-353. The IP tunnels described in Beser permit end devices to directly communicate over a secure and anonymous channel. Ex. 1029 at ¶¶ 278-281, 289-293, 336-339. Beser thus shows "*from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link,*" as specified in **claim 2**. Ex. 1029 at ¶¶ 424-427. Beser thus shows "*sending a message to the network address associated with the secure name of the device using a secure communication link*" as specified by **claim 28**. Ex. 1029 at ¶¶ 609-612. Therefore, Beser anticipates **claims 2 and 28**.

3. Beser Anticipates Claims 24 and 26

As explained above (§ 1) with respect to claims 1 and 29, Beser discloses methods for establishing a secure IP tunneling association between an originating end device and a terminating end device. Thus, for the same reasons presented above with respect to claims 1 and 29 (§ 1), Beser also shows "*A method of using a first device to securely communicate with a second device over a communication network,*" as specified in **claim 24**. Ex. 1029 at ¶¶ 508-515. Beser thus shows "*A method of using a first device to communicate with a second device over a communication network,*" as specified in **claim 26**. Ex. 1029 at ¶¶ 543-545.

Beser describes a configuration where each end device is associated with a phone number, domain name, and public IP address. Ex. 1029 at ¶¶ 290-291, 318-323; *see id.* at ¶¶ 306, 336, 339. In that configuration, Beser shows the phone number can be the unique identifier registered with the trusted-third-party network device, (Ex. 1029 at ¶¶ 306-309, 319-323), while the domain name is a standard domain name registered with a standard name server. Ex. 1029 at ¶¶ 322-323, 379-380; *see id.* at ¶¶ 91-110, 127-133.

Beser explains the trusted-third-party network device can provide a directory service that translates non-standard names, such as E.164 phone numbers, into IP addresses. *See* ¶¶ 284-287, 324-331, *above*. The trusted-third-party network device's directory of subscribers can associate each subscriber's phone number to the IP address of the subscriber's network device and of the subscriber's end

device. *See* ¶ 285. The subscriber's global IP address is unique. Ex. 1029 at ¶ 319. This association necessarily requires the subscriber to have registered its phone number and IP addresses with the trusted-third-party network device. Ex. 1029 at ¶¶ 516-520, 554-558; *see id.* at ¶¶ 306-309, 91-110, 127-133.

Beser explains that, by identifying a user with a static unique identifier, the user can still be located even if the user's IP addresses change because, for example, the user has moved from one office to another. Ex. 1029 at ¶¶ 322-323, 516-520, 554-558. Beser therefore describes a process where users can change IP addresses. For the trusted-third-party network device to be able to associate a unique identifier with the correct IP addresses, each user must register with the trusted-third-party network device whenever the user's IP addresses change. Ex. 1029 at ¶¶ 306-309, 516-520, 554-558. Therefore, for the terminating end device to be listed in the trusted-third-party network device's subscriber directory service, the terminating end device necessarily requested and obtained registration of its unique identifier. *Id.*; *see id.* at ¶¶ 91-110, 127-133.

Beser thus shows "*at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address*" as specified by **claim 24**. Ex. 1029 at ¶¶ 516-521. Beser thus shows "*from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address*

corresponds to the secure name associated with the first device" as specified by **claim 26**. Ex. 1029 at ¶¶ 554-559.

Beser shows that each end device is associated with a domain name is that a standard domain name registered with a standard name server. Ex. 1029 at ¶¶ 322-323, 379-380, 551. Where the device has a domain name listed in a public DNS server, the device necessarily must have registered its domain name and IP address with a DNS server. Ex. 1029 at ¶¶ 91-110, 127-133, 551. Beser thus shows "*from the first device requesting and obtaining registration of an unsecured name associated with the first device*" as specified by **claim 26**. Ex. 1029 at ¶¶ 546-553.

As explained above (§ 1) with respect to claims 1 and 29, Beser shows that the second network device receives a message from the trusted-third-party network device requesting to negotiate private IP addresses and it receives a message from the first network device containing a private IP address. Ex. 1029 at ¶¶ 285, 302-305, 329-339. Each of these messages indicates the originating device desires to communicate securely with the terminating device. Ex. 1029 at ¶¶ 522-529.

For the same reasons as with respect to claims 1 and 29 (§ 1), Beser thus shows "*receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device*" as specified by **claim 24**. Ex. 1029 at ¶¶ 522-529. Beser thus shows "*receiving at the unique network address associated with the secure name a*

message from a second device requesting the desire to securely communicate with the first device" as specified by **claim 26**. Ex. 1029 at ¶¶ 560-568.

As explained above (§ 1) with respect to claims 1 and 29, Beser shows that after the private IP addresses have been assigned, data can be transmitted between the two end devices through a secure and anonymous IP Tunnel. Ex. 1029 at ¶¶ 289-290, 302-305, 336-339. For the same reasons presented above with respect to claims 1 and 29 (§ 1), Beser thus shows "*sending a message securely from the first device to the second device*" as specified by **claim 24**. Ex. 1029 at ¶¶ 530-533. Beser thus shows "*from the first device sending a message securely from the first device to the second device*" as specified by **claim 26**. Ex. 1029 at ¶¶ 569-573. Therefore, Beser anticipates **claims 24 ad 26**.

4. Beser Anticipates Claim 3

Claim 3 depends from claim 2 and further specifies "*the secure name of the second device is a secure domain name*." Beser shows use of many different types of unique identifiers to identify the devices available for an IP tunnel. Ex. 1029 at ¶¶ 318-327. Beser shows the unique identifier can be a domain name. *Id.* Beser shows that if a user attempts to connect to certain domain names, those domain names can be resolved by the trusted-third-party network device and will cause an IP tunnel to be established. Ex. 1029 at ¶¶ 315-338. Therefore, those domain

names are secure domain names. Beser thus anticipates claim 3. Ex. 1029 at ¶¶ 431-435.

5. Beser Anticipates Claim 4

Claim 4 depends from claim 2 and further specifies "*the secure name indicates security*." Beser shows that many different types of unique identifiers can be used to identify the devices available for an IP tunnel. Ex. 1029 at ¶¶ 318-327. Beser shows the unique identifier can be a phone number or another non-standard name. *Id.* A unique identifier that was a dial-up number or non-standard name would indicate security. Ex. 1029 at ¶¶ 441-442. Beser thus anticipates **claim 4**. Ex. 1029 at ¶¶ 441-443.

6. Beser Anticipates Claims 5-6

Claim 5 depends from claim 2 and further specifies the first device receives the message containing the network address associated with the second device "*in encrypted form*." Beser shows systems and processes in which a trusted-third-party network device can be configured to require that communications with it be encrypted. Ex. 1029 at ¶¶ 291-293, 325, 340-353. Any messages sent from the trusted-third-party network device to first network device would be encrypted. Ex. 1029 at ¶¶ 342, 445. Beser thus anticipates c**laim 5**. Ex. 1029 at ¶¶ 445-446.

Claim 6 depends from claim 5 and further specifies the method includes the step of "*decrypting the message*." If the trusted-third-party network device

received an encrypted message, it necessarily would decrypt the message before processing it. Ex. 1029 at ¶¶ 448-449. Similarly, if the first network device received an encrypted message from the trusted-third-party network device, it necessarily would decrypt the message before processing it. Ex. 1029 at ¶ 448. Beser thus anticipates **claim 6**. Ex. 1029 at ¶¶ 447-450.

7. Beser Anticipates Claim 7

Claim 7 depends from claim 2 and further specifies that the second device can support both "*a secure communication link as well as a non-secure communication link*" and a non-secure link is established "*when needed*." Beser shows the terminating device has a private IP address and a public IP address. Ex. 1029 at ¶¶ 322, 336-339, 451. If necessary, the originating device could send packets to the public IP address of the terminating device, and those packets would be routed to the terminating device. Ex. 1029 at ¶¶ 339, 452. Beser thus anticipates **claim 7**. Ex. 1029 at ¶¶ 451-453.

8. Beser Anticipates Claim 8

Claim 8 depends from claim 2 and further specifies the first device receives the message containing the network address associated with the second device "*as an IP address associated with the secure name of the device*." Beser shows that during the negotiation of private IP addresses, the first network device receives a message containing the IP address of the second network device and a message

containing the private IP address for the terminating device. Ex. 1029 at ¶¶ 330-334. The first network device then informs the originating device of the private IP address to be used to communicate with the terminating device. *Id.* Beser thus anticipates **claim 8**. Ex. 1029 at ¶¶ 454-457.

9. Beser Anticipates Claim 9

Claim 9 depends from claim 2 and further specifies the method includes the step of "*automatically initiating the secure communication link after it is enabled*." Where a unique identifier corresponds to a secure terminating device, the trusted-third-party network device will automatically initiate an IP tunnel between the originating and terminating devices by negotiating private IP addresses. Ex. 1029 at ¶¶ 329-336. Negotiation of the IP tunnel is automatic and transparent to the user. Ex. 1029 at ¶¶ 280-282, 329. Beser indicates that IP traffic within an IP tunnel ordinarily will be encrypted utilizing the techniques described in RFC 2401 (*i.e.*, under the IPsec protocol). Encryption of the tunneling connection therefore occurs automatically. Ex. 1029 at ¶¶ 291-293, 325, 342-353. Beser thus anticipates **claim 9**. Ex. 1029 at ¶¶ 458-461.

10. Beser Anticipates Claims 10-11

Claims 10 and 11 depend from claim 2 and further specify the first device receives the message containing the network address associated with the second device "*through tunneling within the secure communication link*" (**claim 10**) or "*in*

the form of at least one tunneled packet" (**claim 11**). Beser shows systems and processes in which communications involving a trusted-third-party network device can be required to be encrypted. Ex. 1029 at ¶¶ 291-293, 325, 340-353. Beser indicates that IP traffic can be encrypted utilizing the techniques described in RFC 2401 (*i.e.*, under the IPsec protocol). Ex. 1029 at ¶¶ 278, 280-281, 291-293, 325, 342-353. Communications sent to and from the trusted-third-party network device could be encrypted and sent via an IPsec tunnel. *Id.* Where IPsec was used to secure those communications, the first network device would receive the public and private IP addresses associated with the terminating end device in tunneled packets. Beser thus anticipates **claims 10 and 11**. Ex. 1029 at ¶¶ 462-465.

11. Beser Anticipates Claim 12

Claim 12 depends from claim 2 and further specifies "*the receiving and sending of messages*" is performed "*in accordance with any one of a plurality of communication protocols*." Beser indicates that terminating network devices can include telephony devices, personal computers, and multimedia devices. Ex. 1029 at ¶ 294. Beser explains that the data that can be transmitted through an IP tunnel can represent VOIP traffic, "multimedia" content (*e.g.*, video, audio), or content for web pages (*e.g.*, delivered to WebTV devices or personal computers). Ex. 1029 at ¶¶ 295-301. The data transmitted through a Beser IP tunnel also can represent video conference traffic or other multimedia content as specified in

H.323. Ex. 1029 at ¶¶ 286, 301. Data transmitted through a Beser IP tunnel can represent data packets of another protocol such as UDP, TCP, SNMP, or TFTP. Ex. 1029 at ¶ 296. Beser thus anticipates **claim 12**. Ex. 1029 at ¶¶ 466-469.

12. Beser Anticipates Claim 13

Claim 13 depends from claim 2 and further specifies "*the receiving and sending of messages*" includes "*multiple sessions*." Beser shows end devices can include telephony devices, personal computers, and multimedia devices. Ex. 1029 at ¶ 294. Beser explains the data transmitted through an IP tunnel can represent VOIP traffic, "multimedia" content (*e.g.*, video, audio), or content for web pages (*e.g.*, delivered to WebTV devices or decoders or personal computers). Ex. 1029 at ¶¶ 295-301. The data transmitted through a Beser IP tunnel also can represent video conference traffic or other multimedia content as specified in H.323. Ex. 1029 at ¶¶ 286, 301. When transmitting multimedia content, each media type (*e.g.*, audio and video) would be transmitted in its own session. Beser thus anticipates **claim 13**. Ex. 1029 at ¶¶ 470-473.

13. Beser Anticipates Claims 14-17

Claim 14 depends from claim 2 and further specifies the method includes the step of "*supporting a plurality of services over the secure communication link*." **Claim 15** depends from claim 14 and further specifies "*wherein the plurality of services comprises a plurality of communication protocols, a plurality of*

application programs, multiple sessions, or a combination thereof." Beser indicates that terminating network devices can include telephony devices, personal computers, and multimedia devices. Ex. 1029 at ¶ 294. Beser explains that the data that can be transmitted through an IP tunnel can represent VOIP traffic, "multimedia" content (*e.g.*, video, audio), or content for web pages (*e.g.*, delivered to WebTV devices or decoders or personal computers). Ex. 1029 at ¶¶ 295-301. The data that is transmitted through a Beser IP tunnel also can represent video conference traffic or other multimedia content as specified in H.323. Ex. 1029 at ¶¶ 286, 301. Data transmitted through a Beser IP tunnel can represent data packets of another service or protocol such as UDP, TCP, SNMP, or TFTP. Ex. 1029 at ¶ 296. Beser thus anticipates **claims 14 and 15**. Ex. 1029 at ¶¶ 474-479.

Claim 16 depends from claim 15 and further specifies "*wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof*." **Claim 17** depends from claim 15 and further specifies "*wherein the plurality of services comprises audio, video or a combination thereof*." Beser explains the data transmitted through an IP tunnel can represent VOIP traffic or "multimedia" content (*e.g.*, video, audio). Ex. 1029 at ¶¶ 295-301. The data transmitted through a Beser IP tunnel also can represent video conference traffic or multimedia content as specified in H.323. Ex. 1029 at ¶¶ 286, 301. Beser thus anticipates **claims 16 and 17**. Ex. 1029 at ¶¶ 474-482.

14. Beser Anticipates Claim 18

Claim 18 depends from claim 2 and further specifies "*the secure communication link is an authenticated link*." Beser shows systems and processes in which a trusted-third-party network device can be configured to require that requests be encrypted and clients be authenticated before it will process a request. Ex. 1029 at ¶¶ 291-293, 325, 340-353. Beser thus anticipates **claim 18**. Ex. 1029 at ¶¶ 483-484.

15. Beser Anticipates Claims 19-20

Claim 19 depends from claim 2 and further specifies "*the first device is a computer, and the steps are performed on the computer*." Beser explains the first network device can be a computer. Ex. 1029 at ¶¶ 282-283, 294-296, 302-305. Beser thus anticipates **claim 19**. Ex. 1029 at ¶¶ 487-488.

Claim 20 depends from claim 2 and further specifies "*the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network*." Beser explains the originating device can be connected to the first network device. Ex. 1029 at ¶ 281. Beser explains the first network device can be a computer connected to a communication network. Ex. 1029 at ¶¶ 277, 282-283, 294-296, 302-305. Beser thus anticipates **claim 20**. Ex. 1029 at ¶¶ 489-491.

16. Beser Anticipates Claim 21

Claim 21 depends from claim 2 and further specifies the method includes the step of "*providing an unsecured name associated with the device*." Beser shows that the terminating device is associated with a secure identifier, such as a phone number. Ex. 1029 at ¶¶ 319-323. Beser also shows the terminating device is associated with unsecure identifiers, such as a domain name and a public IP address. *Id.* Beser thus anticipates **claim 21**. Ex. 1029 at ¶¶ 492-497.

17. Beser Anticipates Claim 22

Claim 22 depends from claim 2 and further specifies "*the secure name is registered prior to the step of sending a message to a secure name service*." Beser explains the trusted-third-party network device can be a standard DNS server. Beser also explains the trusted-third-party network device can provide a directory service that translates non-standard names, such as E.164 phone numbers, into IP addresses. Ex. 1029 at ¶¶ 284-285, 326-331. The trusted-third-party network device's directory of subscribers can associate each subscriber's phone number to the IP address of that subscriber's second network device and the subscriber's IP address. Ex. 1029 at ¶ 285. This association necessarily requires the subscriber to have registered its phone number and IP addresses with the trusted-third-party network device. Ex. 1029 at ¶¶ 306-309, 499-502; *id.* at ¶¶ 91-110, 127-133.

Beser explains that, by identifying a user with a static unique identifier, the user can still be located even if the user's IP addresses change because, for

example, the user has moved from one office to another. Ex. 1029 at ¶¶ 306-309, 499-502. Beser therefore describes a process where users can change IP addresses. *Id.* For the trusted-third-party network device to be able to associate a unique identifier with the correct IP addresses, each user must register with the trusted-third-party network device whenever the user's IP addresses change. *Id.* When an entity registers a domain name with a name server, it specifies the name and one or more addresses to be associated with that name. Ex. 1029 at ¶¶ 91-110, 127-133. Beser thus anticipates **claim 22**. Ex. 1029 at ¶¶ 498-503.

18. Beser Anticipates Claim 23

Claim 23 depends from claim 2 and further specifies "*the secure name of the second device is a secure, non-standard domain name*." As explained above with respect to claim 3 (§ 4), Beser shows that if a user attempts to connect to certain domain names, those domain names will cause an IP tunnel to be established. Ex. 1029 at ¶¶ 315-338. Therefore, those domain names are secure domain names. Beser thus anticipates **claim 23**. Ex. 1029 at ¶¶ 505-506.

19. Beser Anticipates Claim 25

Claim 25 depends from claim 24 and further specifies "*using the first device to obtain a registration of the secure name for the first device*." As explained above with respect to claims 24 and 26 (§ 3), for the terminating end device to be listed in the trusted-third-party network device's subscriber directory service, the

terminating end device necessarily requested and obtained registration of its unique identifier. Ex. 1029 at ¶¶ 91-110, 127-133, 306-309, 537-540. **Claim 25** also specifies that "*sending a message securely comprises sending the message from the first device to the second device using a secure communication link*." As explained above with respect to claims 1 and 29 (§ 1), the transmission of data between the end devices through the IP tunnel satisfies sending a message to from the first device to the second device using a secure communication link. Ex. 1029 at ¶¶ 541-542. Beser thus anticipates **claim 25**. Ex. 1029 at ¶¶ 537-542.

20. Beser Anticipates Claim 27

Claim 27 depends from claim 26 and further specifies "*using the first device to obtain a registration of the unsecured name associated with the first device*" and "*of the secure name associated with the first device*." As explained above with respect to claims 24 and 26 (§ 3), for the terminating end device to be listed in the trusted-third-party network device's subscriber directory service, the terminating end device necessarily requested and obtained registration of its unique identifier. Ex. 1029 at ¶¶ 577-584; *see id.* at ¶¶ 127-133. Where the device has a domain name listed in a public DNS server, the device necessarily registered its domain name and IP address with a DNS name server. Ex. 1029 at ¶¶ 91-110, 127-133, 551. Beser thus anticipates **claim 27**. Ex. 1029 at ¶¶ 577-585.

B. Beser In View of RFC 2401 Renders Obvious Claims 1-29

Claims 1-29 are anticipated by Beser for the reasons set forth in §§ IV.A.1 to A.20, above. Patent Owner may contend Beser does not anticipate these claims for certain reasons. For the reasons presented below, even if Patent Owner's contentions were accepted, a person of ordinary skill in the art would have considered the devices and media defined by claims 1-29 to have been obvious in April of 2000 based on Beser in view of RFC 2401.

1. Claims 1, 2, 24, 26, 28, and 29 Would Have Been Obvious

Claims 1, 2, 24, 26, 28, and **29** each specify the step of sending a message over "*a secure communication link*" or sending a message "*securely*." In proceedings involving other patents in the same family as the '181 patent, Patent Owner has asserted (i) a VPN requires all data sent via the VPN or secure communication link to be encrypted, and (ii) Beser does not teach encryption of all network traffic sent via an IP tunnel. *See, e.g.*, Ex. 1056 at 24-26. Patent Owner may make similar contentions regarding a "secure communication link." Even if those putative distinctions were established, claims 1, 2, 24, 26, 28 and 29 would have been considered obvious based on Beser when considered with RFC 2401.

Initially, Patent Owner's theories about the teachings in Beser and the requirements of the claims are baseless. First, as explained in § III.D.2, above, a "secure communication link" in its broadest reasonable interpretation does not require all network traffic to be encrypted, as secure communication links can be

established using other techniques (e.g., obsfucation). Second, Beser clearly does teach encryption of all traffic sent through an IP tunnel – it states doing so is conventional under the IPSec protocol specified in RFC 2401. Ex. 1029 at ¶¶ 291-293, 342-353. Indeed, Beser makes it clear to a person of ordinary skill that encryption is ordinarily used in IP tunnels, and only suggests possible implementation challenges of doing that in two specific situations involving high volume data transfers and equipment that cannot handle the encryption of that volume of traffic. Ex. 1029 at ¶¶ 291-293, 325, 342-353. Third, Beser does teach use of encryption to establish IP tunnels in the particular applications where Beser suggests that not all network traffic need be encrypted due to practical limitations of a particular computer implementation. Ex. 1029 at ¶¶ 325, 342-353; see also § IV.A.1. For example, Beser shows use of encryption to shield traffic between the trusted-third-party network device and the first and second networks during establishment of the secure IP tunnel. Ex. 1029 at ¶¶ 325, 340-353.

If the Board does not find claims 1, 2, 24, 26, 28, and 29 anticipated by Beser, a person of ordinary skill in the art would have considered those claims to have been obvious, as configuring the Beser IP tunneling scheme to encrypt all network traffic being sent would have been specifically suggested by RFC 2401 (Ex. 1032). Initially, a person of ordinary skill would have considered Beser in conjunction with RFC 2401 – the latter publication defines the IPsec protocol

which Beser expressly states is used to establish conventional IP tunnels. Ex. 1029 at ¶¶ 292-293, 358. A person of ordinary skill would have been motivated to encrypt all traffic sent over an IP tunnel, as this is the practice that Beser identifies is ordinarily followed and which RFC 2401 suggests following. Ex. 1029 at ¶¶ 291-293, 342-353. Thus, the combined teachings of Beser and RFC 2401 would have provided a direct suggestion to encrypt all network traffic being sent through Beser IP tunnels. Ex. 1029 at ¶¶ 354-359, 369-371, 397-399. Indeed, Beser states encryption ordinarily is to be used in IP tunnels, and specifies that the IPsec techniques are to be used for that purpose. Ex. 1029 at ¶¶ 291-293, 342-353. Beser also indicates its IP tunneling schemes are compliant with standards-based processes and techniques (*e.g.*, IPsec), and can be implemented using pre-existing equipment and systems. Ex. 1029 at ¶¶ 282, 286, 306-310, 344, 354-359.

RFC 2401 explains, under the IPsec protocol, network traffic is automatically encrypted as it is sent through security gateways over a public network. Ex. 1029 at ¶¶ 361-371. RFC 2401 shows that, for each tunneling security association, an IPsec header is added to each IP packet (*i.e.*, the packet is placed inside of another packet with an IPsec IP header). Ex. 1029 at ¶¶ 159, 364-368. A person of ordinary skill also would have recognized IPsec could be readily integrated into the Beser systems. Ex. 1029 at ¶¶ 292, 369-370, 400. For example, Beser describes systems that use edge routers and gateways as intermediaries in

transmitting traffic over tunneling associations. Ex. 1029 at ¶¶ 282-283, 302-305, 365-371. RFC 2401 shows precisely the same network configuration described in Beser (*i.e.*, the "case 3" design with network devices on private networks communicating through a tunnel established between edge routers). Ex. 1029 at ¶¶ 362-365, 398-399.

In addition, none of the claims of the '181 patent are limited to the "high volume"/"low equipment capacity" scenarios that were the subject of the Beser cautions. Consequently, any arguments Patent Owner may advance premised on the theory that Beser "teaches away" from using encryption in IP tunnels should be disregarded, as the '181 claims are not limited to situations where that hypothetical concern would be relevant. Moreover, a person of ordinary skill would have immediately recognized there were common sense solutions to the particular capacity problem identified in Beser; namely, use more powerful edge routers or gateway computers or reduce the quality of the digitized voice call or multimedia data to decrease the amount of data that must be encrypted and transferred. Ex. 1029 at ¶¶ 399-401. RFC 2401 also explains its schemes are granular and modular, and the variables in them can be adjusted based on the needs presented by any particular implementation. Ex. 1029 at ¶¶ 369-371, 400-401.

Thus, a person of ordinary skill would have considered encrypting all IP traffic sent in the Beser IP tunneling schemes to have been obvious based on the

guidance in Beser and in RFC 2401, and because it could be implemented by simple and immediately apparent changes to the configuration of the networking environment being used (e.g., by changing the devices to handle greater volumes of encrypted network traffic or by reducing the volume of traffic needing to be sent). Beser considered in view of RFC 2401, thus, would have rendered **claims 1, 2, 24, 26, 28,** and **29** obvious to a person of ordinary skill in the art in April of 2000. Ex. 1029 at ¶¶ 397-401, 429-430, 535, 575, 614, 638.

2. Claims 3-23, 25, and 27 Would Have Been Obvious

If Patent Owner contends that claims 1, 2, 24, 26, 28, and 29 require all network traffic to be encrypted, and that Beser does not teach encryption of all network traffic, these claims on that basis, then Beser considered in view of RFC 2401 would have rendered claims 1, 2, 24, 26, 28, and 29 obvious for the reasons set forth in § 1, above. Also, because Beser itself describes systems and processes meeting all of the requirements of **claims 3-23, 25,** and **27**, each of those claims also would have been considered obvious by a person of ordinary skill in April of 2000 based on the combined teachings of Beser and RFC 2401 for the reasons in §§ A.4, A.5 and A.18, above.

C. Beser In View of Kiuchi Renders Obvious Claims 3-4 and 23

Beser anticipates **claims 3-4 and 23** for the reasons set forth in §§ A.4, A.5 and A.18, above. Patent Owner may contend Beser does not show a secure domain

name or a name that indicates security. The combined teachings of Beser and Kiuchi nonetheless would have rendered claims with this putative distinction obvious. Ex. 1029 at ¶¶ 437-440, 507. Kiuchi shows use of non-standard domain names that can only be resolved by special (non-conventional) nameservers to identify target computers that are located within a closed network. Ex. 1029 at ¶¶ 979-981. A person would have considered Beser with Kiuchi because the two systems share a similar architecture and purpose – both are describing IP tunneling techniques and systems (Ex. 1029 at ¶¶ 281-282, 369, 371, 439, 972-977) and both describe methods of transparently creating a tunneling association between an originating device and a terminating device (Ex. 1029 at ¶¶ 281-282, 361-364, 368-371, 994-998). A person of skill in the art would also recognize that the secure domain name server functionality of Kiuchi could be readily integrated into the Beser scheme (e.g., within or via the trusted-third-party network device). Ex. 1029 at ¶ 440. Therefore, each of **claims 3-4** and **23** would have been obvious to a person of ordinary skill in April of 2000 based on the combined teachings of Beser and Kiuchi. Ex. 1029 at ¶¶ 437-440, 507.

D. Beser In View of RFC 2543 Renders Obvious Claims 22, 24-27

Beser anticipates **claims 22 and 24-27** for the reasons set forth in §§ A.17, A.3 and A.20, above. If Patent Owner contends Beser does not anticipate the claims because it does not show registration of a secure or unsecured name, the

combined teachings of Beser and RFC 2543 would have rendered claims with that putative distinction obvious. Ex. 1029 at ¶¶ 504, 536, 576. RFC 2543 describes the SIP protocol, which is a call signaling technique for initiating VOIP calls. Ex. 1029 at ¶¶ 640-644, 660-662. RFC 2543 describes use of a location server, which allows each user to move between devices and to register its present location so that phone calls always are routed to the correct destination. Ex. 1029 at ¶¶ 666-672. A person of ordinary skill would have combined Beser and RFC 2543 because Beser discloses that its systems can be used with other analogous call signaling protocols. Ex. 1029 at ¶¶ 286, 301; *see id.* at ¶¶ 182-189. That person would have found it obvious to incorporate the SIP registration functionality shown in RFC 2543 into Beser's trusted-third-party network device to enable that device to more efficiently maintain its directory service. Ex. 1029 at ¶¶ 91-110, 127-133, 354-360. Integrating that functionality from RFC 2543 also would have been a simple design choice, combining known technologies with no change in their respective functions to yield predictable results. Ex. 1029 at ¶¶ 504, 536, 576. Therefore, each of **claims 22 and 24-27** would have been considered obvious by a person of ordinary skill in April of 2000 based on the combined teachings of Beser and RFC 2543. Ex. 1029 at ¶¶ 504, 536, 576.

E. Claims 1-6, 8-9, 13-19, and 21-29 Are Anticipated by Kiuchi

Kiuchi is a printed publication that was presented at the 1996 Symposium on Network and Distributed Systems Security (SNDSS) on February 22 & 23, 1996, and published by IEEE in the Proceedings of SNDSS 1996. Kiuchi is a printed publication that was distributed publicly without restriction no later than **February 1996**. *See* Ex. 1011. Kiuchi is prior art to the '181 patent at least under § 102(b). A concise summary of the scheme and processes described in Kiuchi is provided at paragraphs 972 to 998 of Ex. 1029.

1. Claims 1 and 29

Kiuchi describes a method for creating a closed network over the Internet (referred to as the "C-HTTP" system) that allows a user agent (*e.g.*, a web browser) running on a computer in one private network access private web pages (*e.g.*, HTML documents) stored on an origin server located in a different private network. Ex. 1004 at 64, 69. The closed network is constructed over the Internet by using a client-side proxy and a server-side proxy that transparently perform specialized proxy functions for the user agent and the origin server. Ex. 1004 at 64-65. The proxies are installed in firewall devices between the user agent and the origin server, which are unaware of these proxies. *See id.* The user agent, the origin server, and the proxies are conventional HTTP/1.0 compatible devices. *Id.* The client-side proxy and server-side proxy work in conjunction with a C-HTTP name server located on the Internet. *Id.*

Kiuchi describes systems and processes in which a secure connection between a user agent and an origin server is automatically established by proxy servers and a C-HTTP name server in response to a request from a user specifying a secure destination in the closed network. Ex. 1029 at ¶¶ 975, 978, 995-996. Kiuchi shows that an origin server and its server-side proxy can be associated with a domain name resolvable by a public DNS and a secure hostname resolvable by the C-HTTP name server. Ex. 1029 at ¶¶ 978-980. The hostname can be an unconventional domain name such as "Coordinating.Center.CSCRG," which includes the non-standard top-level domain name "CSCRG." Ex. 1029 at ¶ 979. Therefore, Kiuchi shows the origin server and its server-side proxy are associated with a secure and an unsecured name. Ex. 1029 at ¶ 1002, ¶¶ 91-110, 127-133.

Kiuchi shows that the connection process is started when a user agent makes an HTTP request to connect to a hostname that is specified within a URL. Ex. 1029 at ¶¶ 978-980. When the client-side proxy receives the request from the user agent, it sends a request to a C-HTTP name server. Ex. 1029 at ¶¶ 982-983. The C-HTTP name server evaluates the request to determine whether the hostname corresponds to a destination that is part of the closed network and whether the connection between the user agent and the origin server is permitted. Ex. 1029 at ¶¶ 982-987. If the C-HTTP name server determines the hostname in the URL corresponds to a secure destination and that the connection is permitted, it will

return an IP address and other information which allows the client-side proxy to send a message to the server-side proxy. Ex. 1029 at ¶ 988.

Kiuchi thus shows "*A non-transitory machine-readable medium comprising instructions for a method of communicating with a first device associated with a secure name and an unsecured name*" as specified in **claim 1**. Ex. 1029 at ¶¶ 999-1006. Kiuchi thus shows "*A non-transitory machine-readable medium comprising instructions for a method of communicating with a device having a secure name,*" as specified by **claim 29**. Ex. 1029 at ¶¶ 1127-1133.

If C-HTTP server determined the hostname corresponds to a secure destination, ir returns the IP address, public key, and other information corresponding to the hostname. Ex. 1029 at ¶¶ 988-989. The client-side proxy then uses the IP address and key to send an encrypted message to the server-side proxy requesting to make a connection. Ex. 1029 at ¶¶ 988-989. The server-side proxy receives the connection request, and verifies the secure connection is permitted by sending a message to the C-HTTP name server. Ex. 1029 at ¶ 990. Therefore, it receives a message indicating a desire to communicate securely. Ex. 1029 at ¶¶ 1007-1008. If the C-HTTP name server verifies the connection is permissible, the name server will return the IP address and key associated with the client-side proxy, and the server-side proxy accepts the connection. Ex. 1029 at ¶¶ 991-992. Otherwise, the server-side proxy rejects the connection. *Id.*

Kiuchi thus shows "*receiving, at a network address corresponding to the secure name associated with the first device, a message from a second device of the desired to securely communicate with the first device*" as specified in **claim 1**. Ex. 1029 at ¶¶ 1007-1009. Kiuchi thus shows "*receiving at a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered*" as specified by **claim 29**. Ex. 1029 at ¶¶ 1134-1137.

If the C-HTTP name server verifies the received connection request is permissible, the server-side proxy accepts the connection. Ex. 1029 at ¶¶ 990-992. The server-side proxy then sends an encrypted message to the client-side proxy containing a data exchange key. Ex. 1029 at ¶ 991. After the client-side proxy receives the message from the server-side proxy, the connection is established. Ex. 1029 at ¶ 992. The origin server and its proxy can securely transmit data to the user agent and its proxy because the proxy servers will automatically encrypt any traffic sent between them. Ex. 1029 at ¶¶ 992-996. Kiuchi thus shows a method comprising the step of "*sending a message over a secure communication link from the first device to the second device*" as specified in **claim 1**. Ex. 1029 at ¶¶ 1010-1012. Kiuchi thus shows "*sending a message securely from the first device to the*

second device" as specified by **claim 29**. Ex. 1029 at ¶¶ 1138-1140. Thus, Kiuchi anticipates **claims 1 and 29**.

2. Claims 2 and 28

Kiuchi describes systems and processes in which a secure connection between a user agent and an origin server is automatically established by proxy servers and a C-HTTP name server in response to a request from a user specifying a secure destination in the closed network. Ex. 1029 at ¶¶ 975, 978, 995-996. Kiuchi shows that an origin server and its server-side proxy can be associated with a domain name resolvable by a public DNS and a secure hostname resolvable by the C-HTTP name server. Ex. 1029 at ¶¶ 978-980. The hostname can be an unconventional domain name such as "Coordinating.Center.CSCRG," which includes the non-standard top-level domain name "CSCRG." Ex. 1029 at ¶ 979. Therefore, Kiuchi shows the origin server and its server-side proxy are associated with a secure and an unsecured name. Ex. 1029 at ¶ 1016, ¶¶ 91-110, 127-133. Kiuchi thus shows "*A method of using a first device to communicate with a second device having a secure name*" as specified by **claim 2**. Ex. 1029 at ¶¶ 1014-1017. Kiuchi thus shows "*A non-transitory machine-readable medium comprising instructions*," as specified by **claim 28**. Ex. 1029 at ¶¶ 1110-1113.

Kiuchi shows that the process is started when a user agent makes an HTTP request to connect to a hostname that is specified within a URL. Ex. 1029 at

¶¶ 978-980. When the client-side proxy receives the request from the user agent, it sends a request to a C-HTTP name server. Ex. 1029 at ¶¶ 982-983. The C-HTTP name server evaluates the request to determine whether the hostname corresponds to a destination that is part of the closed network and whether the connection between the user agent and the origin server is permitted. Ex. 1029 at ¶¶ 982-987. If the C-HTTP name server determines the hostname corresponds to a secure destination and the connection is permitted, it will return an IP address and other information corresponding to the hostname. Ex. 1029 at ¶ 988. Kiuchi explains the C-HTTP name server is a "secure name service, which contains a certification mechanism . . . [and] is efficient because it can do name resolution and host certification simultaneously." Ex. 1004 at 68 (emphasis added); Ex. 1029 at ¶ 980.

Kiuchi thus shows "*from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device,*" as specified in **claim 2**. Ex. 1029 at ¶¶ 1018-1022. Kiuchi thus shows "*sending a message to a secure name service, the message requesting a network address associated with a secure name of a device*" as specified by **claim 28**. Ex. 1029 at ¶¶ 1114-1118.

If the hostname corresponds to a secure destination, the client-side proxy receives from the C-HTTP name server the IP address, public key, and other information corresponding to the hostname. Ex. 1029 at ¶¶ 988-989. Therefore

the client-side proxy receives the network address associated with the hostname. Ex. 1029 at ¶¶ 1023, 1119. Kiuchi thus shows "*at the first device, receiving a message containing the network address associated with the secure name of the second device,*" as specified in **claim 2**. Ex. 1029 at ¶¶ 1023-1024. Kiuchi thus shows "*receiving a message containing the network address associated with the secure name of the device*" as specified by **claim 28**. Ex. 1029 at ¶¶ 1119-1120.

The client-side proxy then uses the IP address and key to send an encrypted message to the server-side proxy requesting to make a connection. Ex. 1029 at ¶¶ 988-989. Therefore the client-side proxy sends a secure, encrytped message to the network address associated with the hostname. Ex. 1029 at ¶¶ 1025, 1028, 1121. The server-side proxy receives the encrypted connection request, and verifies the secure connection is permitted by sending a message to the C-HTTP name server. Ex. 1029 at ¶ 990. If the C-HTTP name server verifies the connection is permissible, the name server will return the IP address and key associated with the client-side proxy, and the server-side proxy accepts the connection. Ex. 1029 at ¶¶ 991-992. The server-side proxy then sends an encrypted message to the client-side proxy containing a data exchange key. Ex. 1029 at ¶ 991. After the client-side proxy receives the message from the server-side proxy, the connection is established. Ex. 1029 at ¶ 992. The user agent and client-side proxy then can securely send messges to the origin server and server-

side proxy because the proxy servers automatically encrypt any traffic sent between them. Ex. 1029 at ¶¶ 992-996.

Kiuchi thus shows "*from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link*," as specified in **claim 2**. Ex. 1029 at ¶¶ 1025-1029. Kiuchi thus shows "*sending a message to the network address associated with the secure name of the device using a secure communication link*" as specified by **claim 28**. Ex. 1029 at ¶¶ 1121-1125. Thus Kiuchi anticipates **claims 2 and 28**.

3. Claims 24 and 26

As explained above with respect to claims 1 and 29, Kiuchi describes systems and processes in which a secure connection between a user agent and an origin server is automatically established by proxy servers and a C-HTTP name server. Ex. 1029 at ¶¶ 975, 978, 995-996; *see* § 1, *above*. For the same reasons as for claims 1 and 29 (§ 1, *above*), Kiuchi thus shows "*A method of using a first device to securely communicate with a second device over a communication network*," as specified in **claim 24**. Ex. 1029 at ¶¶ 1066-1072. Kiuchi thus shows "*A method of using a first device to communicate with a second device over a communication network*," as specified in **claim 26**. Ex. 1029 at ¶¶ 1087-1093.

Kiuchi shows that before an organization can participate in the closed network, it must install a proxy server and register the proxy's hostname and IP

address with a C-HTTP name server. Ex. 1029 at ¶ 978; Ex. 1004 at 65 ("to participate in a closed network, [an organization] must [] install a client-side and/or server-side proxy on its firewall [and] register an IP address . . . and hostname." (emphasis added)). Kiuchi thus shows "*at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address*" as specified by **claim 24**. Ex. 1029 at ¶¶ 1073-1074. Kiuchi thus shows "*from the first device requesting and obtaining registration of a secure name associated with the first device, wherein a unique network address corresponds to the secure name associated with the first device*" as specified by **claim 26**. Ex. 1029 at ¶¶ 1096-1097.

Kiuchi shows that each host and proxy sever is associated with a domain name resolvable by a public DNS and a secure hostname resolvable by the C-HTTP name server. Ex. 1029 at ¶¶ 978-980; Ex. 1011 (Kiuchi) at 65 (a proxy's "hostname . . . does not have to be the same as its DNS name"). For the domain name to be listed in a public DNS server, it necessarily must have been registered. Ex. 1029 at ¶¶ 1094, 91-110, 127-133. Kiuchi thus shows "*from the first device requesting and obtaining registration of an unsecured name associated with the first device*" as specified by **claim 26**. Ex. 1029 at ¶¶ 1094-1095.

As explained above with respect to claims 1 and 29, Kiuchi explains that after the C-HTTP server returns the server-side proxy's IP address and key, the

client-side proxy transmits a connection request to the server-side proxy. *See* § 1, *above*. Therefore, a message indicating a desire to securely communicate is received at an address associated with the hostname. Ex. 1029 at ¶¶ 988-996.

Thus, for the same reasons as for claims 1 and 29 (§ 1, *above*), Kiuchi shows "*receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device*" as specified by **claim 24**. Ex. 1029 at ¶¶ 1075-1077. Kiuchi thus shows "*receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device*" as specified by **claim 26**. Ex. 1029 at ¶¶ 1098-1100.

As explained above with respect to claims 1 and 29, Kiuchi shows that after the server-side proxy verifies the connection is permitted, it sends an encrypted message to the client-side proxy. *See* § 1, *above*. It also shows that after the connection is established, the server-side proxy and origin server can securely send messages to the client-side proxy and user agent because the proxy servers will automatically encrypt any traffic sent between them. Ex. 1029 at ¶¶ 992-996. For the same reasons as for claims 1 and 29 (§ 1, *above*), Kiuchi thus shows "*sending a message securely from the first device to the second device*" as specified by **claim 24**. Ex. 1029 at ¶¶ 1078-1080. Kiuchi thus shows "*from the first device sending a message securely from the first device to the second device*" as specified by **claim**

26. Ex. 1029 at ¶¶ 1101-1103. Thus, Kiuchi anticipates **claims 24 and 26**.

4. Claims 3-4 and 23

Claims 3, 4, and 23 depend from claim 2 and specify the secure name is "*a secure domain name*" (**claim 3**), "*indicates security*" (**claim 4**), or is "*a secure, non-standard domain name*" (**claim 23**). Kiuchi shows that an origin server and its server-side proxy are associated with a secure hostname resolvable by the C-HTTP name server. Ex. 1029 at ¶¶ 978-980. The hostname can be an unconventional domain name such as "Coordinating.Center.CSCRG," which includes the non-standard top-level domain name "CSCRG." Ex. 1029 at ¶ 979. Use of a non-standard domain name to establish a connection would indicate security. Kiuchi thus anticipates **claims 3, 4, and 23**. Ex. 1029 at ¶¶ 1031-1034, 1064-1065.

5. Claims 5 and 6

Claim 5 depends from claim 2 and further specifies the first device receives the message containing the network address associated with the second device "*in encrypted form*." **Claim 6** depends from claim 5 and further specifies the method includes the step of "*decrypting the message*." If the C-HTTP name server determines a hostname corresponds to a secure destination and that a connection is permitted, it will return to the client-side proxy an IP address corresponding to the hostname. Ex. 1029 at ¶¶ 982-983, 988. The response from the C-HTTP name server is encrypted. Ex. 1029 at ¶ 988. If the client-side proxy receives an

encrypted response from the C-HTTP name server, it necessarily decrypts it. *Id*. Kiuchi thus anticipates **claims 5 and 6**. Ex. 1029 at ¶¶ 1035-1039.

6. Claim 8

Claim 8 depends from claim 2 and further specifies the first device receives the message containing the network address associated with the second device "*as an IP address associated with the secure name of the device*." Kiuchi shows the C-HTTP name server will return an IP address, public key, and other information if it receives a secur ehostname. Ex. 1029 at ¶¶ 988-989. Therefore the client-side proxy receives an IP address associated with the hostname. Ex. 1029 at ¶¶ 1040. Kiuchi thus anticipates **claim 8**. Ex. 1029 at ¶¶ 1040-1041.

7. Claim 9

Claim 9 depends from claim 2 and further specifies the method includes the step of "*automatically initiating the secure communication link after it is enabled*." Kiuchi shows that after the client-side proxy receives the server-side proxy's key, it automatically sends an encrypted message to the server-side proxy. Ex. 1029 at ¶¶ 989, 991, 995-996. Kiuchi shows that after the server-side proxy verifies the connection is permitted, it creates a connection identifier for the session and all communications between the client-side and server-side proxy will be encrypted. Ex. 1029 at ¶ 1043. Kiuchi thus anticipates **claim 9**. Ex. 1029 at ¶¶ 1042-1044.

8. Claim 13

Claim 13 depends from claim 2 and further specifies "*the receiving and sending of messages*" includes "*multiple sessions*." Kiuchi shows the proxy servers can be configured to close the TCP session after each request and response. Ex. 1029 at ¶ 1046. During the course of a secure session, data will be sent using multiple TCP sessions. Ex. 1029 at ¶¶ 1045-1046; Ex. 1025 at 18:42-46. Kiuchi thus anticipates **claim 13**. Ex. 1029 at ¶¶ 1045-1047.

9. Claims 14-17

Claim 14 depends from claim 2, and claim 15 from claim 14. **Claim 14** specifies the method of claim 2 includes the step of "*supporting a plurality of services over the secure communication link*" and **claim 15** further specifies "*the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof*." Claims 16 and 17 each depends from claim 15. **Claim 16** specifies "*wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof*" and **claim 17** specifies "*wherein the plurality of services comprises audio, video or a combination thereof*".

Kiuchi explains that its system is built on HTTP because of its flexibility in permitting "distributed multimedia information systems with user-friendly graphical interfaces." Ex. 1029 at ¶ 997. This flexibility allows the system to "provide services similar to those which have been provided by [other] protocols,"

such as "FTP, SMTP, NNTP, GOPHER." *Id.*; Ex. 1004 at 67. Kiuchi explains that any type of data that transmitted via HTTP can be sent through its systems, such as electronic mail, HTML documents, and multimedia. Ex. 1029 at ¶ 997. Kiuchi thus anticipates **claims 14 to 17**. Ex. 1029 at ¶¶ 1048-1053.

10. Claim 18

Claim 18 depends from claim 2 and further specifies "*the secure communication link is an authenticated link.*" The C-HTTP name server authenticates the request using a digital signature and then evaluates it to determine whether the connection is permitted. Ex. 1029 at ¶¶ 981, 983-984. Kiuchi shows that the server-side proxy also authenticates the connection by asking the C-HTTP name server to confirm that a client-side proxy is part of the closed network. Ex. 1029 at ¶¶ 981, 990. Kiuchi thus anticipates **claim 18**. Ex. 1029 at ¶¶ 1054-1056.

11. Claim 19

Claim 19 depends from claim 2 and specifies "*the first device is a computer, and the steps are performed on the computer*." Kiuchi shows the connection process is peformed by the client-side proxy on behalf of the user agent. Ex. 1029 at ¶¶ 1014-1029. Kiuchi thus anticipates **claim 19**. Ex. 1029 at ¶¶ 1057-1059.

12. Claim 21

Claim 21 depends from claim 2 and adds the step of "*providing an unsecured name associated with the device.*" Kiuchi shows that each host and proxy sever is associated with a domain name resolvable by a public DNS and a

secure hostname resolvable by the C-HTTP name server. Ex. 1029 at ¶¶ 978-980. Therefore, each device is provided with a public domain name. Ex. 1029 at ¶¶ 1060-1061. Kiuchi thus anticipates **claim 21**. *Id.*

13. Claim 22

Claim 22 depends from claim 2 and further specifies "*the secure name is registered prior to the step of sending a message to a secure name service*." Kiuchi shows that before an organization can participate in the closed network, it must register a hostname with C-HTTP name server. Ex. 1029 at ¶¶ 978, 985; *see* § 3, *above*. Kiuchi thus anticipates **claim 22**. Ex. 1029 at ¶¶ 1062-1063.

14. Claim 25

Claim 25 depends from claim 24 and further specifies "*using the first device to obtain a registration of the secure name for the first device*." Kiuchi shows that before an organization can participate in the closed network, it must install a proxy server and register that proxy server's hostname and IP address with C-HTTP name server. Ex. 1029 at ¶¶ 978; *see id.* at ¶¶ 91-110, 127-133.

Claim 25 also specifies that "*sending a message securely comprises sending the message from the first device to the second device using a secure communication link*." As explained above with respect to claims 1 and 29, Kiuchi shows that after the server-side proxy verifies the connection is permitted, it sends an encrypted message to the client-side proxy. *See* § E.1, *above*. It also shows that

after the connection is established, the server-side proxy and origin server can securely send messages to the client-side proxy and user agent because the proxy servers will automatically encrypt any traffic sent between them. Ex. 1029 at ¶¶ 992-996. Kiuchi thus anticipates **claim 25**. Ex. 1029 at ¶¶ 1082-1086.

15. Claim 27

Claim 27 depends from claim 26 and further specifies "*using the first device to obtain a registration of the unsecured name associated with the first device*" and "*of the secure name associated with the first device*." Kiuchi shows that each host and proxy sever is associated with a domain name resolvable by a public DNS and a secure hostname resolvable by the C-HTTP name server. Ex. 1029 at ¶¶ 978-980. For the domain name to be listed in a DNS server, it necessarily must have been registered. Ex. 1029 at ¶¶ 1105, 91-110, 127-133. Before an organization can participate in the closed network, it must install a proxy server and register that proxy server's hostname and IP address with the C-HTTP name server. Ex. 1029 at ¶ 978. Kiuchi thus anticipates **claim 27**. Ex. 1029 at ¶¶ 1105-1109.

V. CONCLUSION

Because the information presented in this petition shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition, the Petitioner respectfully requests that a Trial be instituted and that claims 1-29 be canceled as unpatentable.

Dated: March 10, 2014

Respectfully Submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

PETITION FOR INTER PARTES REVIEW

OF U.S. PATENT NO. 8,051,181

ATTACHMENT A:
PROOF OF SERVICE OF THE PETITION

CERTIFICATE OF SERVICE

I hereby certify that on this 10th day of March, 2014, a copy of this Petition, including all attachments, appendices and exhibits, has been served in its entirety by Federal Express on the following counsel of record for patent owner:

Joseph E. Palys
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
11955 Freedom Drive
Reston, VA 20190-5675
Phone: (571) 203-2700
Fax: (202) 408-4400
E-mail: joseph.palys@finnegan.com

Naveen Modi
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
901 New York Avenue, NW
Washington, DC 20001-4413
Telephone: (202) 408-4065
Facsimile: (202) 408-4400
E-mail: naveen.modi@finnegan.com

Dated: March 10, 2014

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Reg. No. 43,401
Attorney for Petitioner

PETITION FOR INTER PARTES REVIEW

OF U.S. PATENT NO. 8,051,181

ATTACHMENT B:
LIST OF EVIDENCE AND EXHIBITS RELIED UPON IN PETITION

Exhibit #	Reference Name
1001	U.S Patent No. 7,188,180
1002	File History of U.S Patent No. 7,188,180
1003	U.S. Patent No. 6,557,037 ("Provino")
1004	Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP - The Development of a Secure, Closed HTTP-based Network on the Internet," published by IEEE in the Proceedings of SNDSS 1996
1005	Alvaro Guillen *et al.*, 1993 International Conference on Network Protocols, *An Architecture for Virtual Circuit/QoS Routing* (Oct. 1993) ("Guillen")
1006	Dave Kosiur, *Building and Managing Virtual Private Networks* (1998) ("Kosiur")
1007	U.S. Patent No. 6,151,628 to Xu *et al.* ("Xu")
1008	U.S. Patent No. 6,073,175 to Tavs *et al.* ("Tavs")
1009	U.S. Patent No. 6,225,993 to Lindblad *et al.* ("Lindblad")
1010	U.S. Patent No. 8,200,837 to Bhatti *et al.* ("Bhatti")
1011	Declaration of Dr. Roch Guerin ("Guerin Declaration")
1012	[RESERVED]
1013	Dismissal from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:10CV94
1014	Copy of Docket from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:10CV94
1015	[RESERVED]
1016	Claim Construction Opinion and Order from *VirnetX, Inc. v. Microsoft Corp.*, Docket No. 6:07CV80
1017	Joint Claim Construction Chart Pursuant To P.R. 4-5(d), *VirnetX Inc., vs. Cisco Systems, Inc.*, Docket No. 6:10-CV-417
1018	Claim Construction Opinion and Order from *VirnetX Inc., vs. Cisco Systems, Inc.*, Docket No. 6:10-CV-417
1019	E. Gavron, RFC 1535, *A Security Problem and Proposed Correction With Widely Deployed DNS Software* (Oct. 1993)
1020	RFC 791, *Internet Protocol* (Sep. 1981)

Exhibit #	Reference Name
1021	T. Berners-Lee *et al.*, RFC 1945, *Hypertext Transfer Protocol -- HTTP/1.0* (May 1996)
1022	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, 9 Digital Technical Journal 2 (1997)
1023	Excerpts from the Prosecution History of Reexamination Control No. 95/001,270
1024	Excerpts from the Prosecution History of Reexamination Control No. 95/001,792
1025	U.S Patent No. 8,051,181
1026	File History of U.S Patent No. 8,051,181
1027	U.S Patent No. 7,987,274
1028	File History of U.S Patent No. 7,987,274
1029	Declaration of Michael Fratto re: U.S. Patent No. 8,051,181
1030	Micheal Fratto CV
1031	U.S. Patent No. 6,496,867 to Beser
1032	Kent, S., et al., RFC 2401, "Security Architecture for the Internet Protocol," November 1998
1033	H. Schulzrinne et al., RFC 2543, "SIP: Session Initiation Protocol," March 1999
1034	Schulzrinne, H., et al., RFC 1889, "RTP: A Transport Protocol for Real-Time Applications," January 1996
1035	Handley, M., et al., RFC 2327, "SDP: Session Description Protocol," April 1998
1036	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987
1037	Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987
1038	Srisuresh, P., et al., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999
1039	Tittel, E., et al., Windows NT Server 4 for Dummies, Ch. 12, pp. 191-210 (1999)

Exhibit #	Reference Name
1040	Microsoft Press, "Microsoft Windows 98 Resource Kit, The Professional's Companion to Windows 98," Ch. 9, pp. 355-396, Ch. 15, and Ch. 19, pp. 849-918 (1998)
1041	Aventail AutoSOCKS v2.1 Administration and User's Guide, 1996-1997
1042	Aventail Connect v3.1/v2.6 Administrator's Guide, 1996-1999
1043	Ferguson, P. and Huston, G., "What Is a VPN? – Part I," The Internet Protocol Journal, Vol. 1, No. 1 (June 1998)
1044	Ferguson, P. and Huston, G., What Is a VPN? – Part II," The Internet Protocol Journal, Vol. 1, No. 2 (September, 1998)
1045	Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989
1046	Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997
1047	Socolofsky, T., et al., RFC 1180, "A TCP/IP Tutorial," January 1991
1048	U.S. Patent No. 4,405,829 to Rivest et al.
1049	Rescorla, E., et al., RFC 2660, "The Secure HyperText Transfer Protocol," August 1999
1050	Lloyd, B., et al., RFC 1334, "PPP Authentication Protocols," October 1992
1051	Simpson, W., RFC 1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," August 1996
1052	Dierks, T., et al., RFC 2246, "The TLS Protocol – Version 1.0," January 1999
1053	Simpson, W., RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994
1054	Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996
1055	Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September 1998
1056	Pall, G., RFC 2118, "Microsoft Point-To-Point Compression (MPPC) Protocol," March 1997
1057	Gross, G., et al., RFC 2364, "PPP Over AAL5," July 1998
1058	Townsley, W.M., et al., RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999

Exhibit #	Reference Name
1059	Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993
1060	Adams, C., et al., RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols," March 1999
1061	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3," October 1996
1062	Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996
1063	Malkin, G., RFC 2453, "RIP Version 2," November 1998
1064	Moy, J., RFC 2328, "OSPF Version 2," April 1998
1065	Vixie, P., et al., RFC 2136, "Dynamic Updates in the Domain Name System (DNS Update)", April 1997
1066	VirnetX's Opening Claim Construction Brief in VirnetX Inc. v. Cisco Systems, Inc., et al., 6:10-CV-417 (11/4/11) (EDTX)
1067	Defendants' Responsive Claim Construction Brief in VirnetX Inc. v. Cisco Systems, Inc., et al., 6:10-CV-417 (12/7/11) (EDTX)
1068	VirnetX's Reply Claim Construction Brief in VirnetX Inc. v. Cisco Systems, Inc., et al. , 6:10-CV-417 (12/19/11) (EDTX)
1069	[RESERVED]
1070	Joint Claim Construction and Prehearing Statement in VirnetX Inc. v. Apple Inc., 6:12-CV-855 (2/14/14)
1071	International Trade Commission, Investigation No. 337-TA-858, Parties' Joint List of Disputed Claim Terms (2/25/13)
1072	File History of *Inter Partes* Reexamination of 8,051,181, Control No. 95/000,949
1073	U.S. Patent No. 6,182,141 to Blum
1074	U.S. Patent No. 6,701,437 to Hoke
1075	E. Wedlund & H. Schulzrinne, "Mobility Support Using SIP," WOWMOM '99 Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia
1076	Record of Publication of WOWMOM (Ex. 1015) on ACM Digital Library (available at http://dl.acm.org/citation.cfm?id=313281)
1077	ITU-T Recommendation H.323 (February 1998)
1078	U.S. Patent No. 6,430,176 to Christie

Exhibit #	Reference Name
1079	WAP Forum, Wireless Application Protocol Architecture Specification (April 30, 1998)
1080	W3C, "World Wide Web Consortium and Wireless Application Protocol Forum Establish Formal Liaison Relationship, " December 8, 1999
1081	IBM Session Initiation Protocol (SIP)
1082	Gulbrandsen, A., et al., RFC 2052, "A DNS RR for specifying the location of services (DNS SRV)," October 1996
1083	ITU-T H.225-0, "Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems," (February 1998)
1084	ITU-T H.235, "Security and Encryption for H-Series (H.323 and other H.245-Based) Multimedia Terminals," (November 1998)
1085	ITU-T H.245, "Infrastructure of Audiovisual Services – Communication Procedures," (February 1998)
1086	U.S. Patent and Trademark Office, Right of Appeal Notice, Reexamination Control No. 95/001,788
1087	U.S. Patent and Trademark Office, Right of Appeal Notice, Reexamination Control No. 95/001,789