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. 8,850,009
Issued: September 30, 2014
Filed: June 6, 2013
Inventors: Victor Larson, *et al.*
Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inter Partes Review No. IPR2015-00812

Petition for *Inter Partes* Review of
U.S. Patent No. 8,850,009

Table of Contents

I. Introduction

A. Certification the '009 Patent May Be Contested by Petitioner

Petitioner certifies that U.S. Patent No. 8,850,009 (Ex. 1003) (the '009 patent) is available for *inter partes* review. Petitioner also certifies it is not barred or estopped from requesting *inter partes* review of the claims of the '009 patent. Neither Petitioner, nor any party in privity with Petitioner, has filed a civil action challenging the validity of any claim of the '009 patent. The '009 patent has not been the subject of a prior *inter partes* review by Petitioner or a privy of Petitioner.

Petitioner also certifies this petition for *inter partes* review is timely filed as it has never been asserted against Petitioner in litigation. Thus, because there is no patent owner's action, this petition complies with 35 U.S.C. § 315(b). Petitioner also notes that the timing provisions of 35 U.S.C. § 311(c) and 37 C.F.R. § 42.102(a) do not apply to the '009 patent, as it pre-dates the first-to-file system. *See* Pub. L. 112-274 § 1(n), 126 Stat. 2456 (Jan. 14, 2013).

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 in 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))

IPR2015-00813 filed concurrently also involves the ’009 patent. Each petition advances unique grounds and are based on different primary references. IPR2015-00813 challenges claims **1-8, 10-20 and 22-25** of the ’009 patent on obviousness grounds based on “Aventail Connect v3.01/v2.51 Administrator’s Guide” (Ex. 1009) alone or in combination with “RFC 2543; SIP: Session Initiation Protocol” (Ex. 1013) or “Request for Comments: 2401; Security Architecture for the Internet Protocol” (Ex. 1008). These references show that the Aventail VPN system for creating virtual private networks using encrypted and authenticated connections, alone or in combination with the SIP protocol or the IPsec protocol, would have rendered obvious the DNS-based systems and methods for establishing an encrypted communication link according to the ’009 claims.

The present petition and IPR2015-00813 present unique correlations of the challenged ’009 claims to the prior art, and each warrants independent institution of trial. Petitioner respectfully requests the Board institute each petition, as each presents distinct and non-redundant grounds.

3. Lead and Backup Lead Counsel (§ 42.8(b)(3))

Lead Counsel is: Jeffrey P. Kushan (Reg. No. 43,401), jkushan@sidley.com, (202) 736-8914. Back-Up Lead Counsel are: Scott Border (*pro hac* to be requested), sborder@sidley.com, (202) 736-8818; and Thomas A. Broughan III

(Reg. No. 66,001), tbroughan@sidley.com, (202) 736-8314.

4. Service Information (§ 42.8(b)(4))

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

5. 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 1-8, 10-20 and 22-25 of the ’009 patent are unpatentable for being obvious under 35 U.S.C. § 103 based on U.S. Patent No. 6,496,867 to Beser (“Beser”) (Ex. 1007) in view of “RFC 2401, Security Architecture for the Internet Protocol,” (“RFC 2401”) (Ex. 1008) and the knowledge of a person of ordinary skill in the art. A list of evidence relied upon in support of this petition is set forth in **Attachment B**.

III. Relevant Information Concerning the Contested Patent

A. Overview of the ’009 Patent

1. The ’009 Patent Specification

The ’009 patent is a member of a family of patents issued to Larson et al., including, *inter alia*, U.S. Patent Nos. 6,502,135 (“ ’135 patent”), 7,188,180 (“ ’180 patent”), 7,418,504 (“ ’504 patent”), 7,490,151 (“ ’151 patent”), 7,921,211 (“ ’211 patent”), 7,987,274 (“ ’274 patent”), 8,051,181 (“ ’181 patent”), 8,504,697

(“ ’697 patent”), and 8,868,705 (“ ’705 patent”).[1]

The ’009 patent disclosure, like other members of this patent family, is largely focused on techniques for securely communicating over the Internet based on a protocol called the “Tunneled Agile Routing Protocol” or “TARP.” Ex. 1003 at 3:20-23. According to the ’009 specification, TARP allows for secure and anonymous communications by using tunneling, an IP address hopping scheme where the IP addresses of the end devices and routers participating in the system can change over time, and a variety of other security techniques. Ex. 1003 at 1:38-40, 3:20-6:13. Two short sections of the ’009 specification – spanning primarily columns 39 to 42 and 49 to 53 – are directed to a different concept, namely, techniques for establishing secure communications in response to DNS requests specifying a secure destination. *See* Ex. 1003 at 39:36-42:29, 49:41-53:49. This material was added in a continuation-in-part application filed in February 2000. In proceedings involving related patents, Patent Owner has asserted that these short passages provide written description support for claim terms involving domain names, DNS requests, requests to look up network addresses, and DNS servers.

These portions of the ’009 specification describe a “conventional DNS server” that purportedly is modified to include additional functionality that allows

---

[1] IPR2015-00810 and -00811 filed concurrently involve the ’705 patent.

it to support the creation of virtual private networks. *See* Ex. 1003 at 40:29-57. According to the '009 specification, the "modified DNS server" (*id.* at 40:33-34) receives a request to look up a network address associated with a domain name, determines whether a secure site has been requested (for example, by checking an internal table of sites), and then performs additional steps to support establishing a "virtual private network" with the secure site. *See* Ex. 1003 at 39:33-38, 40:11-28, 40:39-57, 41:31-49, 52:7-13. This process can include conventional devices such as personal computers running web browsers, proxy servers, intermediate routers, and web servers. Ex. 1003 at 40:29-38, 49:55-65, 52:65-53:4.

The '009 specification describes several optional features of this system, such as using "IP hopblocks" to create a VPN or incorporating user authentication. Ex. 1003 at 40:18-22, 40:27-28, 41:42-49, 52:21-34. It also describes several optional configurations of the "modified DNS server," including a standalone DNS server and a system incorporating a DNS server, a DNS proxy server, and a gatekeeper. Ex. 1003 at 41:1-14.

2. Representative Claims

Independent claims 1 and 14 of the '009 patent define a network device and a method, respectively, but recite the same operative steps. *See* Ex. 1003 at 56:22-48, 57:22-58:3. Claim 14 is representative, specifying a method executed by a first network device for communicating with a second network device by: (1) sending a

request to look up a network address of the second network device; (2) receiving, following interception of the request, (i) an indication that the second network device is available for a secure communications service; (ii) the requested network address; and (iii) provisioning information for an encrypted communication link; (3) connecting to the second network device over the encrypted communication link; and (4) communicating data using the secure communications service via the encrypted communication link, the first network device being a device at which a user uses the secure communications service to access the encrypted communication link.

B. Patent Owner's Assertion of Related Patents

Patent Owner has asserted varying sets of claims of its patents in this family against Petitioner and other entities in numerous lawsuits. In August of 2010, Patent Owner sued Petitioner and five other entities (the "2010 Litigation") asserting claims from the '135, '151, '504, and '211 patents. In November 2011, Patent Owner filed a lawsuit accusing Petitioner of infringing claims of the '181 patent. In December 2012, Patent Owner served a new complaint on Petitioner asserting infringement of numerous claims of the '135, '151, '504, and '211 patents (the "2012 Litigation"). In August 2013, Patent Owner served an amended complaint adding the '697 patent to the 2012 Litigation. Patent Owner also asserted patents from this family against Microsoft and others in separate lawsuits

filed in February 2007, March 2010, and April 2013, and against numerous other defendants in actions filed in 2010 and 2011.

C. Effective Filing Date

The ’009 patent issued from U.S. Appl. No. 13/911,792 (“the ’792 application”). The ’792 application claims the benefit as a continuation of the following applications: 13/903,788, filed May 28, 2013; 13/336,790 (issued as U.S. Patent No. 8,458,341); 13/049,552 (issued as U.S. Patent No. 8,572,247); 11/840,560 (issued as the ’211 patent); 10/714,849 (issued as the ’504 patent); and 09/558,210, filed April 26, 2000, and now abandoned. It also is designated a **continuation-in-part** of 09/504,783, filed on February 15, 2000 (“the ’783 application”), which is a **continuation-in-part** of 09/429,643, filed on October 29, 1999. The ’210, ’783 and ’643 applications also claim priority to 60/106,261, filed October 30, 1998 and 60/137,704, filed June 7, 1998.

Claims 1 and 14 of the ’009 patent are independent claims. Claims 2-8 and 10-13 depend directly or indirectly from **claim 1**, and claims 15-20 and 22-25 depend directly or indirectly from **claim 14**. Claims 2-8, 10-13, 15-20 and 22-25 cannot enjoy an effective filing date earlier than that of claims 1 and 14, respectively, from which they depend.

Claims 1 and 14 of the ’009 patent rely on information found only in the ’783 application. For example, claim 1 of the ’009 patent specifies a network

device comprising at least one processor configured to execute an application program to enable the network device to "send a ***domain name service (DNS) request***…" and "receive, following interception of the ***DNS request***…" (emphasis added). Claim 14 specifies a method executed by a first network device comprising "sending a ***domain name service (DNS) request***…" and "receiving, following interception of the ***DNS request***…" (emphasis added). No application filed prior to the '783 application mentions the terms "domain name," "domain name service" or "DNS request," much less provide a written description of devices or methods corresponding to the '009 patent claims. In proceedings involving the related '135, '504, '151, '211, '274 and '697 patents, Patent Owner has not disputed that claims reciting a "domain name" or "domain name service" are not entitled to an effective filing date prior to February 15, 2000. *See*, *e.g.*, Patent Owner Preliminary Oppositions in IPR2013-00348, -00349, -00354, -00375 to -00378, -00393, -00394, -00397, and -00398, as well as IPR2014-00237, -00238, -00403, -00404, and -00610; *see also Inter Partes* Reexamination Nos. 95/001,682, 95/001,679, 95/001,697, 95/001,714, 95/001,788, and 95/001,789. Accordingly, the effective filing date of the '009 patent claims is no earlier than **February 15, 2000**.

D. The Person of Ordinary Skill in the Art

A person of ordinary skill in the art in the field of the '009 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. 1005 ¶ 110.

E. Claim Construction

In this proceeding, claims must be given their broadest reasonable construction in light of the specification. 37 CFR § 42.100(b). The ’009 patent shares a common disclosure and uses several of the same terms as the ’697, ’274, ’180, ’151, ’504, and ’211 patents with respect to which Patent Owner has advanced constructions. Also, if Patent Owner contends terms in the claims should be read as having 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 any

district court litigation, which employs a different claim construction standard.

1. "domain name service (DNS) request"

Each independent claim recites the term "***domain name service (DNS) request***." The '009 patent does not define the term "domain name service (DNS) request. In IPR2014-00610 involving the related '151 patent, the Board has interpreted "DNS request" to mean "a request for a resource corresponding to a domain name." Paper 9 at 6 (Oct. 15, 2014). This is consistent with the '009 patent specification, which provides examples of DNS requests seeking to obtain a network address corresponding to a "web name" or "domain name." Ex. 1003 at 39:39-45, 40:52-58; *see also* Ex. 1005 at ¶ 85. Accordingly, the broadest reasonable interpretation of "domain name service (DNS) request" is "***a request for a resource corresponding to a domain name***." Ex. 1005 at ¶ 85.

2. "interception of the DNS request"

Each independent claim requires "***interception of a DNS request***." In a related proceeding involving the '697 patent, the Board interpreted the phrase "intercepting . . . a request" as including "receiving a request pertaining to a first entity at another entity." IPR2014-00237, Paper 15 at 13 (May 14, 2014). The Board further explained that "intercepting" a request involves "receiving and acting on" a request, the request being "intended for" receipt at a destination other than the destination at which the request is intercepted. *Id.* at 12. The Board's

construction is consistent with the ’009 patent specification. Ex. 1005 at ¶ 67.

The ’009 patent does not expressly define “interception” of a DNS request, but uses the term “intercepting” as meaning receiving a request at a device other than the device specified in the request. Ex. 1005 at ¶ 68, 86. For example, the specification explains that a DNS proxy 2610 “intercepts” all DNS lookup functions to examine whether access to a secure site has been requested. Ex. 1003 at 40:39-45, Figs. 26 & 27. The specification also shows the requests are routed to the DNS proxy instead of a DNS server 2609, which ordinarily would receive and resolve the domain name in the request. *Id.* at 39:39-41. Because the DNS proxy and DNS server as described as separate entities, the ’009 patent uses the term “intercept” as meaning receipt of a message by a proxy server instead of the intended destination. Accordingly, the broadest reasonable interpretation of the term “interception of the DNS request” includes “***receiving a DNS request pertaining to a first entity at another entity***.” Ex. 1005 at ¶ 86.

3. “encrypted communication link”

Each independent claim recites the term “***encrypted communication link***.” The ’009 patent does not define “encrypted communication link.” The Board has not interpreted this term in proceedings involving related patents, but has construed the terms “secure communication link” and “virtual private network communication link.” Specifically, in IPR2014-00237 involving the related ’697

patent, the Board interpreted "secure communication link" to mean "a transmission path that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." Paper 15 at 10 (May 4, 2014). Also, in IPR2014-00481 involving the related '180 patent, the Board interpreted "virtual private network communication link" to mean "a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." Paper 11 at 6-7 (Sept. 3, 2014).

Like the '697 and '180 patent claims, the '009 patent claims require communication over a "communication link," but the '009 claims specify that the link is "encrypted." All three patents generally claim DNS-based methods and systems for establishing secure communications or VPNs. The common specification explains that the DNS-based VPN scheme permits computers to privately communicate with each other over a public network by protecting their anonymity. *See* Ex. 1003 at 39:56-65. In other words, the "communication link" resulting from implementation of the claimed DNS-based methods and systems must be "a transmission path that restricts access to data, addresses, or other information on the path, including, but not limited to, one or more of

authentication, encryption, or address hopping." Ex. 1005 at ¶¶ 88-90; *see also* IPR2014-00237, Paper 15 at 10 (May 4, 2014); IPR2014-00481, Paper 11 at 6-7 (Sept. 3, 2014). Thus, an "encrypted communication link" is a type of secure communication link that uses encryption. Ex. 1005 at ¶ 90. The broadest reasonable interpretation of "encrypted communication link" in the context of the '009 claims is "***a transmission path that restricts access to data, addresses, or other information on the path at least by using encryption***." Ex. 1005 at ¶ 91.

4. "provisioning information"

Each independent claim recites the term "***provisioning information***." The '009 patent does not define "provisioning information." The only discussion in specification concerning "provisioning" states that "VPN gatekeeper 3314 *provisions* computer 3301 and secure web server computer 3320, or a secure edge router for server computer 3320, thereby creating the VPN." Ex. 1003 at 52:10-13 (emphasis added). The '009 specification also explains that, after a DNS proxy determines that access a secure site has been requested, it transmits a message to a gatekeeper requesting creation of a "virtual private network." *Id.* at 40:45-48, 41:39-42. The gatekeeper returns a resolved IP address and IP address "hopblocks" to be used by the client computer and the target site to communicate securely. *Id.* at 40:48-57; *see also* Ex. 1005 at ¶ 74.

In IPR2014-00481 involving the '180 patent, whose claims recite

provisioning information for a "virtual private network" rather than "encrypted communications channel," the Board interpreted "provisioning information" as "information that is provided to enable or to aid in establishing communications to occur in the VPN." Paper 11 at 11 (Sept. 3, 2014). The '009 patent disclosure only describes use of DNS systems to establish VPN connections between devices, and it does not describe creating encrypted channels that are isolated from a VPN. *See* Ex. 1003 at 39:36-38, 51:31-33, 52:9-10, Fig. 37. Examples of "provisioning information" in the '009 patent includes IP address hopblocks or other data that enables or to aids in establishing communications in a VPN where the VPN uses encryption. Ex. 1003 at 40:45-57: Ex. 1005 at ¶ 75. Therefore, the broadest reasonable interpretation of the term "provisioning information" in the context of the '009 claims is "***information that enables communication in a virtual private network, where the virtual private network uses encryption***." Ex. 1005 at ¶ 92.

5. "secure communications service"

Each independent claim recites the term "***secure communications service***." The '009 patent does not expressly define this term. In IPR2014-00237 involving the related '697 patent, the Board interpreted the term "secure communications service" as "the functional configuration of a network device that enables it to participate in a secure communication link with another network device." Paper 15 at 10 (May 14, 2014). "Secure communication link" in turn has been interpreted

by the Board to mean "a transmission path that restricts access to data, addresses, or other information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." IPR2014-00237, Paper 15 at 10 (May 4, 2014).

This is consistent with the '009 patent specification, which uses the phrase "secure communications service" in a manner that indicates the term simply refers to the capacity of two computers to participate in a secure communications link. Ex. 1005 at ¶ 95. For example, the '009 patent explains that a first network device "communicat[es] at least one of video data and audio data with the second network device using the secure communications service via the secure communication link." Ex. 1003 at 8:28-31, 8:45-48. Therefore, the broadest reasonable construction of the term "secure communications service" should encompass "***the functional configuration of a network device that enables it to participate in a secure communications link with another computer or device***." Ex. 1005 at ¶ 96.

6. "indication"

Each independent claim requires the first network device to receive "an indication" that the second network device is available for the secure communications service. The '009 specification does not define the term "indication." In IPR2014-00614 involving the related '504 patent, the Board interpreted the term "indication" to mean "something that shows the probable

presence or existence or nature of." Paper 9 at 12-13 (Oct. 15, 2014); *see also* IPR2014-00615, Paper 9 (Oct. 15, 2014) (involving the related '211 patent).

This is consistent with the '009 specification, which explains that, after a DNS proxy determines access to a secure site has been requested and forwards the request to a gatekeeper, the client receives a "resolved" address and is provisioned information such as "hopblocks" to be used for secure communication with the secure target site. Ex. 1003 at 40:39-57; Ex. 1005 at ¶ 99. In some scenarios, the DNS proxy may return a "host unknown" error message, such as if the user lacks appropriate credentials. Ex. 1003 at 40:62-65. Although a web browser may show an icon indicating a secure connection has been established (*id.* at 52:37-40), the '009 specification contains no discussion of a client receiving a message explicitly confirming that the secure target site is available for secure communications. Ex. 1005 at ¶ 100. Accordingly, the broadest reasonable interpretation of the term "indication" should encompass "***something that shows the probable presence or existence or nature of.***" Ex. 1005 at ¶ 101.

7. "virtual private network communication link"

Dependent claims 8 and 21 specify that the encrypted communication link "is part of a ***virtual private network communication link***." The '009 patent does not provide an explicit definition for "virtual private network communication link." In IPR2014-00481 involving the related '180 patent, the Board interpreted "virtual

private network communication link" to mean "a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping." Paper 11 at 6-7 (Sept. 3, 2014). The Board also read the '180 patent as employing various levels of security in a VPN that do not require encryption, such as authentication, or information or address hopping. *Id.* at 7.

This is consistent with the '009 specification, which explains that "software module 3309 accesses secure server 3320 through VPN communication link 3321" and the communication link 3321 is shown as only the portion of the path between computer 3301 and server 3320 that is over network 3302. Ex. 1003 at 52:35-36, Fig. 33; Ex. 1005 at ¶ 104. Accordingly, the broadest reasonable interpretation of "virtual private network communication link" is "***a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping***." Ex. 1005 at ¶ 105.

8. "domain name"

Dependent claims 7 and 20 recite the term "***domain name***." The '009 patent does not define "domain 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. 1005 at ¶ 70. A more general description of "domain name" has been advanced by Patent Owner in other proceedings; namely, "a name corresponding to an IP address." *See, e.g.*, Ex. 1042 at 14-15. Both definitions are reasonable; thus the broadest reasonable interpretation of "domain name" is "***a name corresponding to an IP address***." Ex. 1005 at ¶ 106.

9. "modulation"

Dependent claims 4, 5, 17 and 18 recite the term "***modulation***." The term "modulation" is not defined in the '009 patent. In IPR2014-00237 involving the '697 patent, the Board interpreted "modulation" to include "the process of encoding data for transmission over a medium by varying a carrier signal." Paper 15 at 14 (May 14, 2014). This is consistent with the '009 patent and the understanding of a person of ordinary skill in the art. Ex. 1005 at ¶¶ 78-79 . For example, the specification explains that transmission paths may comprise "logically separate paths contained within a broadband communication medium (*e.g.*, separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link)." Ex. 1003 at 35:17-23. A person of skill would understand "unmodulated" and "modulated" to refer to whether data is encoded for transmission over a physical medium by varying or "modulating" a carrier signal.

Ex. 1005 at ¶ 80. Any data transmitted via a modem (*i.e.*, a "modulator-demodulator" device) is modulated. *Id*. Similarly, any data transmitted via a cellular network is modulated. *Id*. Accordingly, the broadest reasonable interpretation of "modulation" is "***the process of encoding data for transmission over a medium by varying a carrier signal***." Ex. 1005 at ¶ 108.

IV. Analysis of the Patentability of the '009 Patent

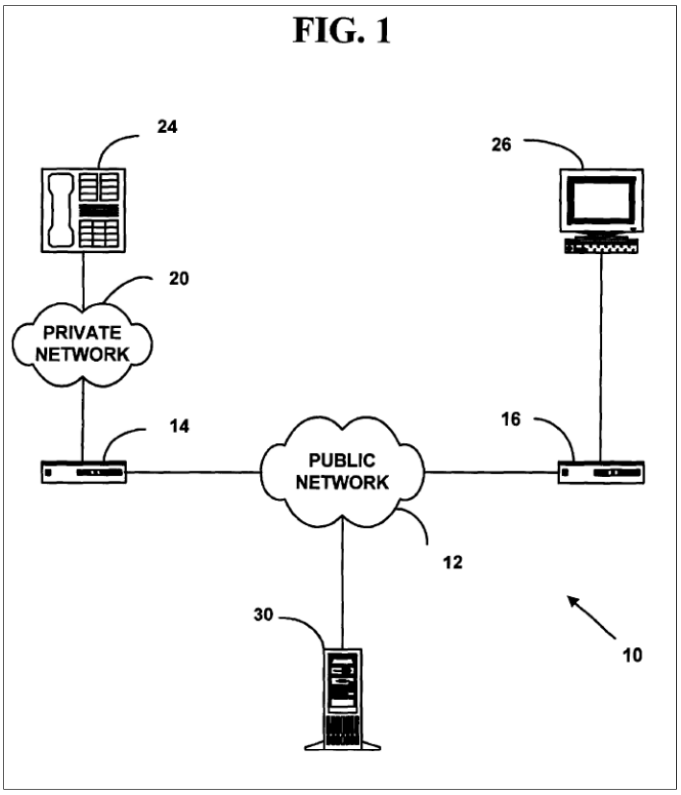
The '009 patent has two independent claims (claims 1 and 14), each of which specifies the same operative steps. *See* § III.A.2. Claim 14 is representative, and as explained above, defines a process where a first network device communicates with a second network device via an encrypted communication link after a DNS request to look up a network address of the second device is intercepted.

A. Overview of Beser (Ex. 1007)

Beser (Ex. 1007) was filed on **August 27, 1999**, and is prior art to the '009 claims under 35 U.S.C. § 102(e). Ex. 1007 at 1. The operation and features of the Beser system are explained in greater detail in Ex. 1005 at ¶¶ 274-345.

Beser describes methods and systems for establishing an IP tunneling association between originating (24) and terminating (26) end devices, with the aid of a first network device (14), a second network device (16), and a trusted-third-party network device (30). Ex. 1007 at 2:46-67. Fig. 1 provides an illustrative

embodiment for the invention disclosed in Beser:



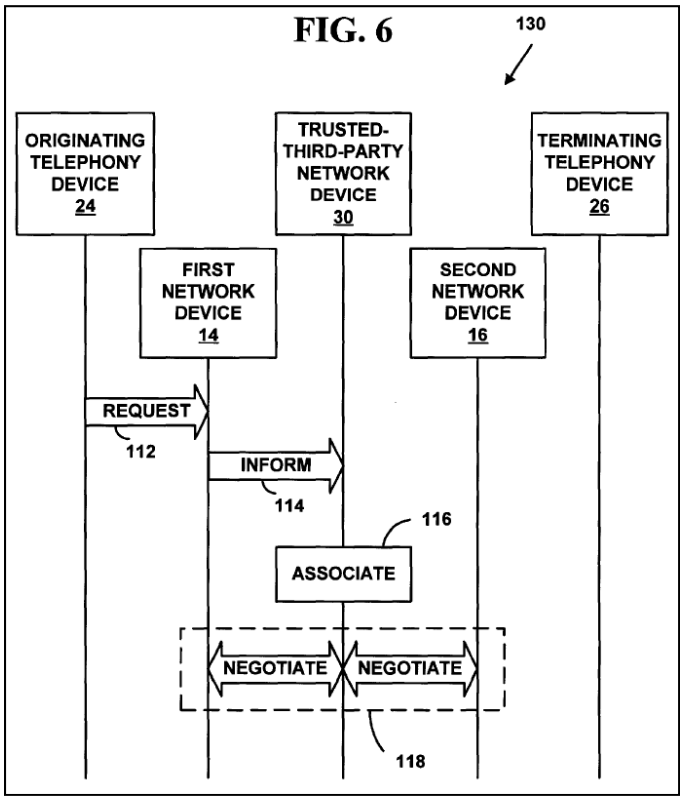
Id. at Fig. 1.

Beser explains that the originating and terminating end devices can be telephony devices (including portable "VoIP devices" and "personal computers running facsimile or audio applications") or multimedia devices (such as "Web-TV sets [], interactive video game players, [and] personal computers running multimedia applications"). *Id*. at 4:43-52. The first and second network devices may be edge routers, "gateway" computers, cable modems, or other network devices. *Id*. at 4:7-42. Beser further explains that the trusted-third-party network device can be "a back-end service, a domain name server, or the owner/manager of

database or directory services." *Id*. at 4:9-11. As Beser explains, its system is intended to be integrated into conventional network devices and configurations. *Id*. at 4:55-5:2; Ex. 1005 at ¶¶ 282-83, 285.

a) Request Containing a Unique Identifier

To establish an IP tunneling association in the Beser scheme, the originating end device sends a request containing a "unique identifier" specifying a destination (*i.e.*, a terminating end device). Ex. 1007 at 7:63-8:3. This is illustrated in Fig. 6:



Id. at Fig. 6.

Beser teaches that many types of identifiers can be used for the unique identifier, but that in one preferred embodiment, the unique identifier is a domain

name. *Id*. at 10:37-41; Ex. 1005 at ¶ 276, 318-19. As an example of the Beser system, a VoIP application running on a portable telephony device could initiate an IP tunnel by sending out a request that included a domain name associated with the terminating end device. Ex. 1007 at 4:50-52, 10:55-66; Ex. 1005 at ¶ 320. As another example, the request could be sent by a personal computer running a multimedia application or a web browser, and it could include a domain name of the web server containing multimedia content as the unique identifier. Ex. 1007 at 4:47-54, Fig. 1; Ex. 1005 at ¶ 320. Other examples of unique identifiers include email addresses and E.164 compliant telephone numbers. Ex. 1007 at 10:37-11:5; Ex. 1005 at ¶ 276.

Next, the first network device receives the request, evaluates it to determine whether it is a tunneling request, and if so, sends it to the trusted-third-party network device. Ex. 1007 at 8:21-52; Ex. 1005 at ¶¶ 299-300, 317, 322. Otherwise, the first network device processes the request normally, such as by sending it to a conventional DNS server. Ex. 1007 at 4:7-42; Ex. 1005 at ¶ 300, 317, 322. Beser shows that one way the first network device can determine whether to send the request to the trusted-third-party network device is by checking the datagram for a distinctive sequence of bits indicating that it is part of a tunneling association. Ex. 1007 at 8:34-47; Ex. 1005 at ¶ 299-300. If the datagram does not contain this distinctive sequence indicating the request should

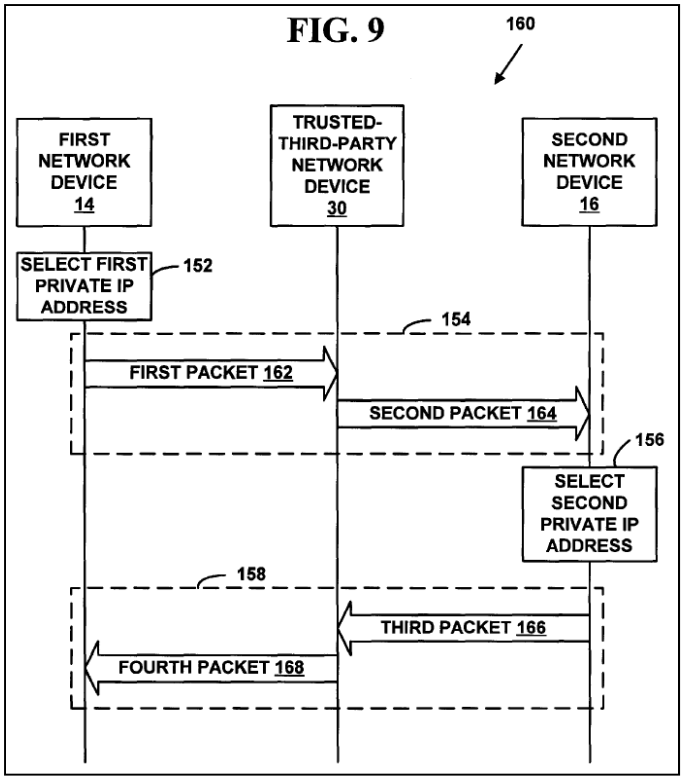
be re-directed to the trusted third party network device, it will be handled by ordinary procedures. Ex. 1005 at ¶ 309.

However, if the request contains the distinctive sequence, it is re-directed to the trusted-third-party network device, which receives and evaluates the request and determines whether it corresponds to a terminating end device that can communicate using an IP tunnel. Ex. 1007 at 9:6-11, 11:26-58; Ex. 1005 at ¶¶ 309-10, 322. Beser explains that the trusted-third-party network device can be a DNS server, and it can be modified to contain a database of unique identifiers (*e.g.*, domain names, e-mail addresses or phone numbers) associated with devices or users that participate in the Beser scheme. Ex. 1007 at 4:9-11, 11:26-58; Ex. 1005 at ¶¶ 276-77, 307-08, 323. As Beser explains, the database contains the list of authorized devices, and each entry in the database includes the unique identifier, the "IP 58 address of a particular second network device 16," and the "public IP 58 addresses for the terminating telephony device 26." Ex. 1007 at 11:48-52. A person of ordinary skill in the art would understand that the trusted-third-party network device determines whether the unique identifier (*e.g.*, domain name) is associated with a device that can communicate using a secure IP tunnel by checking this internal database of eligible devices. Ex. 1005 at ¶¶ 323-25; Ex. 1007 at 11:48-52. If the trusted-third-party network device determines that a tunneling association may be established with the terminating end device, the

trusted-third-party network device negotiates with the first and second network devices to facilitate the exchange of private IP addresses. Ex. 1007 at 9:6-11, 9:26-30; Ex. 1005 at ¶¶ 278, 301, 311, 324.

b) Negotiation of Private IP Addresses

In the Beser scheme, the trusted-third-party network device negotiates private IP addresses for the originating and terminating end devices by communicating with the first and second network devices over a public network. Ex. 1007 at 9:26-30, 11:59-64; Ex. 1005 ¶ 333. In the negotiation, each network device selects a private IP address for its end device and provides that address to the trusted-third-party network device. Ex. 1007 at 13:10-29, 13:66-14:18; *see id.* at 13:10-14:33; Ex. 1005 at ¶¶ 336, 338. The trusted-third-party network device sends a message to the second network device that contains the originating end device's private IP address and the first network device's public IP address. Ex. 1007 at 13:38-42; Ex. 1005 at ¶¶ 336-37. It also sends a message to the first network device that contains the terminating end device's private IP address and the second network device's public IP address. Ex. 1007 at 14:19-27; Ex. 1005 at ¶¶ 338-39. This is depicted in Fig. 9:



Ex. 1007 at Fig. 9.

This process protects the identity of the end devices because the exchanged IP packets contain only public addresses for the first, second, and trusted-third-party network devices in the "source" and "destination" address fields. *Id.* at 13:13-18, 13:33-38; Ex. 1005 at ¶ 335. Beser explains that, following negotiation, each network device has the private IP addresses of both the originating and terminating end devices. Ex. 1007 at 14:51-62. Beser also explains "the private network addresses [are transmitted] to the network devices at the ends of the tunneling association where the private network addresses are stored on these end devices." *Id*. at 21:48-52. The private IP addresses for the originating and terminating end devices will be used to establish a virtual tunneling association and

transmit data between the end devices over a public network, providing anonymity. *Id*. at 8:12-20, 11:59-62, 12:28-32; Ex. 1005 at ¶¶ 342-44. "[A]ny packet sent from the originating network device 24 to the first network device 14 may include the private network addresses of the originating and terminating ends of the tunneling association." Ex. 1007 at 21:55-58.

Beser's scheme employs standard IP packets to establish an IP tunnel. *Id*. at 7:7-26; Ex. 1005 at ¶ 334. Beser also explains that data traffic within an IP tunnel ordinarily will be encrypted according to the IPsec protocol, where encryption of the tunneling connection occurs automatically. Ex. 1007 at 1:54-56, 2:6-14; 11:22-25; Ex. 1005 at ¶¶ 385-87*; see also* Ex. 1008. The IPsec protocol, described in RFC 2401 (Ex. 1008), was well-known to those of skill in the art, and a person of ordinary skill would have been able to readily configure IPsec to provide encryption services within the Beser scheme.

B. Overview of RFC 2401 (Ex. 1008)

RFC 2401 (Ex. 1008) was published in **November 1998**, and is prior art to the '009 patent under 35 U.S.C. § 102(b). Ex. 1008 at 1. The operation and features of the systems described in RFC 2401 are explained in greater detail in Ex. 1005 at ¶¶ 346-364.

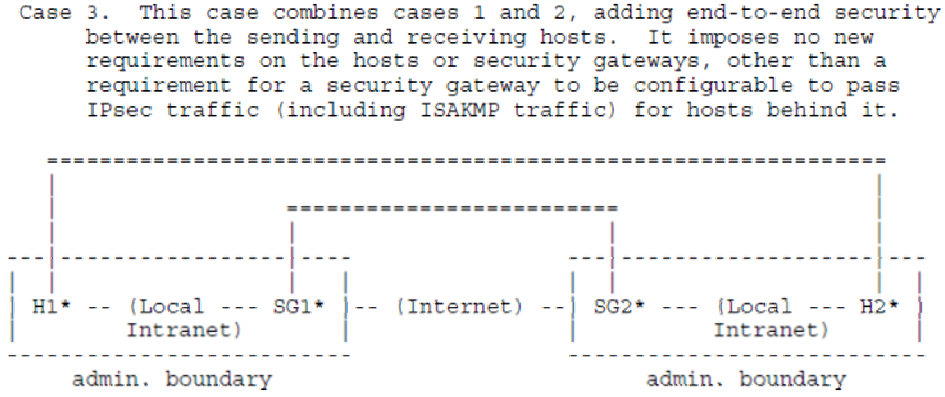
RFC 2401 describes the IPsec protocol promulgated by the Internet Engineering Task Force (IETF). RFC 2401 explains that IPsec can be used to

protect one or more "paths" between a pair of hosts, between a pair of security gateways (*e.g.*, a router or firewall), or between a security gateway and a host. Ex. 1008 at 6; Ex. 1005 at ¶ 348. RFC 2401 teaches that IPsec can be integrated into existing network configurations, such as via edge routers or gateway network devices, and end devices such as client computers or web servers. Ex. 1008 at 7-8; Ex. 1005 at ¶ 348. RFC 2401 shows that IPsec can be implemented in "transport" or "tunnel" modes, which allow protection to be applied to upper layer protocols and tunneled IP packets, respectively. Ex. 1008 at 7; Ex. 1005 at ¶¶ 353-55.

RFC 2401 explains that, using the IPsec protocol, network traffic is automatically encrypted as it is sent through security gateways over a public network. Ex. 1008 at 30; Ex. 1005 at ¶¶ 356, 361. In this scheme, IPsec compliant devices evaluate all IP traffic to determine whether encryption is required for each packet and, if so, the packet is placed inside of an IPsec packet and encrypted. Ex. 1008 at 30; Ex. 1005 at ¶¶ 356, 361.

RFC 2401 describes several configurations in which encryption is implemented between hosts or security gateways according to IPsec. Ex. 1008 at 24-26; Ex. 1005 at ¶¶ 363-64. RFC 2401 shows that IPsec can be used to provide encryption over certain portions of a communications path, or they can be used to provide end-to-end encryption. Ex. 1008 at 24-26; Ex. 1005 at ¶¶ 363-64. In one configuration, RFC 2401 shows one tunnel between two security gateways such as

edge routers, and another encrypted tunnel between the two end devices:



Ex. 1008 at 25.

C. Beser (Ex. 1007) In View of RFC 2401 (Ex. 1008) Would Have Rendered Obvious Claims 1-8, 10-20 and 22-25

Patent Owner is likely to contend, as it has in other proceedings involving related patents, that Beser does not teach or suggest an "encrypted communications link" because Beser teaches that streaming audio or video data may be securely transferred over Beser IP tunnels in unencrypted form. *See* Ex. 1007 at 1:58-67. But, as explained elsewhere in this petition, Beser clearly teaches that this is only one example of an application of Beser's scheme, and that data sent via an IP tunnel is and should ordinarily be encrypted. Ex. 1007 at 1:54-56, 2:6-14; *see also* 11:22-25, 18:2-5, 20:11-14. Beser also refers to the IPSec protocol as the conventional way of establishing such secure IP tunnels, which a person of ordinary skill would consult to implement the Beser IP tunneling scheme. Ex. 1007 at 1:54-56.

To minimize the disputed issues in this proceeding and thereby enable a

focused and efficient review of the '009 patent claims, Petitioner has framed the patentability question in this petition against the non-encrypted streaming audio/video example described in Beser. Even if only that particular example in Beser is considered, it would have rendered the claims of the '009 patent unpatentable as having been obvious to a person of ordinary skill in view of RFC 2401 (Ex. 1008).[2] In this petition, Petitioner explains why this is the case. First, it posits this as the putative distinction between the claimed methods and systems relative to the unencrypted streaming audio/video data example in Beser. The petition then explains why a person of ordinary skill would have considered configuring the Beser scheme to support encryption of streaming audio/video data to have been an obvious design choice based on Beser in view of the guidance in RFC 2401. The combined teachings of Beser with RFC 2401 are then compared to each element of the independent claims. This comparison shows that the design, elements and arrangement of the Beser system correspond precisely to the systems

---

[2] As explained in this and other proceedings, Beser teaches more than this streaming audio/video example. This disclosure in Beser consequently anticipates claims in several of Patent Owner's patents specifying simply establishment of a secure communication link or secure communications. *See*, IPR2014-00237, -00238, -00483, -00484.

described in the '009 patent which are claimed in method and system form. In that analysis, the sole possible distinction between the claims and the Beser streaming data example is a question of configuration of the Beser components to provide "end-to-end" encryption of the traffic being sent over the IP tunnel. The petition explains why configuring Beser in this manner would have been considered an obvious design choice to the person of ordinary skill in the art well before 2000, based on the guidance in RFC 2401. Beser in view of RFC 2401 would have rendered claims 1 and 14 obvious to a person of ordinary skill.

1. A Person of Ordinary Skill Would Have Found It Obvious to Encrypt IP Traffic in the Beser Scheme Based on the Teachings in Beser and RFC 2401

Initially, a person of ordinary skill would have considered the teachings of Beser in conjunction with those in RFC 2401 because Beser expressly refers to the IPsec protocol (which is defined in RFC 2401) as being the conventional way that the IP tunnels described in Beser are established. Ex. 1007 at 1:54-56; Ex. 1005 at ¶¶ 383-85, 395. For example, Beser explains that a "sender may encrypt the information inside the IP packets before transmission, e.g., with IP Security ('IPSec')." Ex. 1007 at 1:54-56. Beser also indicates that 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. *Id*. at 4:55-5:2; Ex. 1005 at ¶¶ 282-83, 285, 386, 394, 398. That indication and others in Beser

would have led the person of ordinary skill to consider the guidance in RFC 2401 when considering how to implement the Beser scheme. Ex. 1005 at ¶¶ 385, 388-90, 395, 398-403.

Beser also teaches that IP tunnels are and should ordinarily be encrypted. Ex. 1007 at 1:54-56, 11:22-25, 18:2-5; Ex. 1005 at ¶¶ 383-85, 389-90. Indeed, Beser teaches the person of ordinary skill that in its scheme, encryption should be used – even in the data streaming example. For instance, Beser explains that packets sent during establishment of a tunnel should be encrypted, even for the data streaming examples. As it states, certain "IP 58 packets may require encryption or authentication to ensure that the unique identifier cannot be read on the public network 12." Ex. 1007 at 11:22-25; *see also id.* at 18:2-5; 20:11-14.

Thus, a person of ordinary skill would have understood that standard techniques, such as IPsec, can and should be used to implement the Beser scheme, as this is the practice that Beser identifies is conventionally followed. Ex. 1005 at ¶¶ 389, 393; Ex. 1007 at 1:54-56, 2:12-14; *see also* 11:22-25, 18:2-5, 20:11-14. In particular, a person of ordinary skill would have been specifically motivated to encrypt IP traffic within the IP tunnel of Beser pursuant to the guidance in RFC 2401, which describes the IPsec protocol referenced in Beser. Ex. 1005 at ¶¶ 389-390, 393, 399; Ex. 1007 at 1:54-56; *see also* Ex. 1008.

A person of ordinary skill also would have also recognized IPsec could be

readily integrated into the Beser systems. Ex. 1005 at ¶¶ 391-92, 398-400. For example, Beser describes systems that use edge routers and gateways as intermediaries in transmitting traffic over tunneling associations, which is one of the network designs shown in RFC 2401. Ex. 1007 at 4:7-8, 4:18-29. Indeed, RFC 2401 in its "case 3" example shows precisely the same network topology as Beser, with one tunnel between two security gateways such as edge routers, and another tunnel between the two end devices. *Compare* Ex. 1008 at 25 *with* Ex. 1007 at Fig. 1; Ex. 1005 at ¶¶ 396-97. When Beser is configured in this manner, it would use the IPSec case 3 design to provide end-to-end encryption, hiding the data, while the Beser IP tunnel would provide anonymity over the public network, hiding the true source and destination addresses. Ex. 1005 at ¶ 399.

Patent Owner may contend Beser teaches away from implementing its scheme by encrypting the IP traffic pursuant to the teachings of RFC 2401. But Beser does not "teach away" from using IPSec – it does not say encryption cannot be used to transmit streaming data. Rather, Beser indicates that use of encryption in these unique situations *may* cause challenges. Ex. 1007 at 1:58-65; Ex. 1005 at ¶¶ 387-89. This type of observation does not "teach away" from the combination of Beser and RFC 2401 under applicable law. The Federal Circuit has explained:

> … obviousness must be determined in light of all the facts, and there is no rule that a single reference that teaches away will mandate a finding of nonobviousness. Likewise, a given course of action often

> has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.

Medichem, SA v. Rolabo, SL, 437 F. 3d 1157, 1165 (Fed. Cir. 2006).

Indeed, several passages of Beser plainly indicate that encryption should be used and criticize prior art techniques that prevent use of end-to-end encryption. Ex. 1007 at 2:22-27, 11:22-25, 18:2-5, 20:11-14. Moreover, the implementation challenges that Beser identifies in using encryption in data streaming applications would have been seen by a person of ordinary skill as implicating simple trade-offs – increasing or limiting the quality of the streaming video or audio data, or using less or more powerful equipment. Ex. 1005 at ¶¶ 388-390. In addition, the IPsec protocol was known to be highly adaptable, enabling it to accommodate computational burdens of a particular configuration by adjusting parameters of the IPsec protocol (*e.g.*, adjusting the strength or type of encryption used). *See* Ex. 1008 at 4, 7, 10. More significantly, a person of ordinary skill would face no technical challenges in implementing the Beser scheme to encrypt streaming audio or video data. For example, a person of ordinary skill would have immediately recognized that using more powerful edge routers or gateway computers, or reducing the quality of the digitized voice call or multimedia data, would decrease the amount of data that must be encrypted, thereby enabling IPsec encryption to be used even in streaming video or audio applications of Beser. Ex. 1005 at ¶¶ 389-

90. Accordingly, a person of ordinary skill would have considered Beser in conjunction with RFC 2401 in February 2000. Ex. 1005 at ¶¶ 393, 399. When so considered, the person of ordinary skill would have found it obvious to encrypt the IP traffic being sent over the Beser secure IP tunnel, even in the streaming video or audio applications discussed in Beser. Ex. 1005 at ¶¶ 389, 393, 399.

2. Independent Claims 1 and 14 Would Have Been Obvious

Claims 1 and 14 are defined using the same operative limitations. *See* Ex. 1003 at 56:22-48, 57:22-58:3. Claim 14 is cast in the form of a method for two devices to communicate through a secure communications service and encrypted communication link; claim 1 is cast in the form of a network device configured to execute the steps of the method defined in claim 14. In this analysis, the steps of the method claim (claim 14) are first addressed, followed by the corresponding system elements of claim 1.

a) Claim 14 Preamble

The preamble of claim 14 specifies "*a method executed by a first network device for communicating with a second network device*." Beser describes a method for establishing an IP tunnel between an originating end device ("*first*

network device")[3] and a terminating end device ("*second network device*"). Ex. 1007 at 8:15-20, 21:52-62, 22:2-22; Ex. 1005 at ¶¶ 274, 342-43. The process described in Beser begins when a user sends a request through the originating end device by, for example, entering the website destination of a WebTV source, or initiating a VoIP call. Ex. 1007 at 4:43-54, 7:64-66, 10:22-36, 10:55-66; Ex. 1005 at ¶¶ 316, 320, 345. The request is processed by the trusted-third-party network device which, with the help of the first and second network devices, establishes a private tunneling association between the end devices, enabling the originating end device to communicate with the terminating end device. Ex. 1007 at 8:15-20, 14:51-67; Ex. 1005 at ¶¶ 278, 324, 335-40. Beser thus describes "*a method executed by a first network device for communicating with a second network device*" as specified in **claim 14**.

b) "send[ing]. . . a domain name service (DNS) request to look up a network address . . . based on an identifier . . ."

Both **claims 1 and 14** specify a first step where the first network device sends a "*domain name service (DNS) request*" to look up a network address of a second network device. The request must be "*based on an identifier associated*

---

[3] Claim 1 specifies a "network device" instead of a "first network device." For simplicity, the references to the "first network device" of claim 14 in this analysis are intended to apply equally to the "network device" of claim 1.

with the second network device." In the Beser scheme, the originating end device ("*first network device*") sends a request to initiate a tunneling association with a terminating end device. Ex. 1007 at 7:64-8:1, 9:64-10:41; Ex. 1005 at ¶ 316. This request contains a unique identifier that is associated with the terminating end device ("*the second network device*"). Ex. 1007 at 8:1-3, 10:37-11:8; Ex. 1005 at ¶ 318. The unique identifier can be a domain name, and the trusted-third-party network device that processes the request can be a domain name server. Ex. 1007 at 4:9-11, 10:37-42, 10:55-11:5; Ex. 1005 at ¶ 319. Beser thus shows a "*domain name service (DNS) request*" (*i.e.*, a request for a resource corresponding to a domain name). According to the '009 patent, a DNS request can include a "web name" or "domain name." *See* Ex. 1003 at 39:39-45, 40:39-45. An "identifier" in the context of the '009 claims therefore encompasses a domain name. In Beser, the unique identifier can be a domain name ("*an identifier associated with the second network device*"). Ex. 1007 at 10:37-42, 10:55-11:5; Ex. 1005 at ¶ 319.

In Beser, after receiving the request, the trusted-third-party network looks up the public IP address associated with the unique identifier and negotiates private IP addresses for the originating and terminating end devices. Ex. 1007 at 11:26-36, 11:45-58, 12:28-32, 17:42-49; Ex. 1005 at ¶¶ 323-25. Following the negotiation, the originating end device receives the private IP address associated with the terminating end device ("*a network address of a second network device*"). Ex.

1007 at 14:51-62, 21:48-52; Ex. 1005 at ¶ 340. Beser thus shows a "*domain name service (DNS) request*" because the tunneling request is "a request for a resource corresponding to a domain name" (*i.e.*, a request to establish an IP tunnel with the terminating end device corresponding to the domain name unique identifier). Ex. 1005 at ¶ 85. Therefore, Beser shows a system and method that perform the first step specified in **claims 14 and 1**.

c) The "receiving" step

The second step of **claims 1 and 14** is compound, and it specifies receiving a set of information following "interception of the DNS request" and a determination that the second network device is available for secure communications. Each sub-part is address below.

(1) Receiving, following "interception of the DNS request"

The second step of **claims 1 and 14** specifies "*interception of the DNS request*." In Beser, when the originating end device sends out the request to initiate a tunneling association with a terminating device ("*DNS request*"), the request is received by the first network device, which evaluates all of the data packets it receives (*i.e.*, the request is "intercepted" by the first network device). Ex. 1007 at 8:21-47; Ex. 1005 at ¶¶ 299-300, 317, 322. If the first network device determines that a data packet contains a request to initiate an IP tunnel (*e.g.*, due to the presence in it of a distinctive sequence of bits in the datagram), it will forward

the packet to the trusted-third-party network device for special processing. Ex. 1007 at 8:21-47; Ex. 1005 at ¶ 322. Otherwise, it processes the packet normally, such as by sending it to a conventional DNS server. Ex. 1007 at 4:7-42, 8:39-44; Ex. 1005 at ¶ 300.

After the trusted-third-party network device receives ("*intercepts*") the request containing the domain name ("*DNS request*"), it looks up the IP address associated with the domain name. Ex. 1007 at 4:8-11, 8:4-7, 10:38-41, 11:26-55; Ex. 1005 at ¶¶ 310, 323-25. Beser thus shows that, even though the request contains a unique identifier associated with the terminating end device, the request is actually "intercepted" by each of the first network device and the trusted-third-party network device. Ex. 1007 at 8:21-47; Ex. 1005 at ¶ 86. Accordingly, Beser shows interception of a DNS request as specified in **claims 1 and 14**.

(2) Receiving, following " . . . a determination that the second network device is available for a secure communications service. . ."

Both **claims 1 and 14** specify that a "*determination that the second network device is available for the secure communications service*" is made. The '009 patent does not define "determination," but the specification explains that a DNS proxy can "determine" whether access to a secure site has been requested "by reference to an internal table of [secure] sites." Ex. 1003 at 40:39-45; *see also* IPR2014-00237 Paper 15 at 15 (May 14, 2014) (defining "determining . . . whether

the second network device is available for a secure communications" as including one or more of "1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester.").

Beser shows a "*determination*" as specified in the claims. Beser explains that the trusted-third-party network device can be a domain name server that functions according to industry standards (Ex. 1007 at 4:55-63, 11:32-36), but is modified to maintain a database correlating each registered unique identifier to "the IP 58 address of a particular second network device 16" and may also include "public IP 58 addresses for the terminating telephony device 26." Ex. 1007 at 11:48-52; *see also* 11:26-44; Ex. 1005 at ¶¶ 323, 325, 327. Beser teaches that the trusted-third-party network device determines whether the unique identifier in a request specifies a destination that can establish a secure tunnel by checking its internal database of registered users or devices. Ex. 1007 at 11:30-36, 11:45-58; Ex. 1005 at ¶¶ 310, 323, 325, 327. This is the same type of "determination" disclosed in the '009 patent. *See* Ex. 1003 at 40:39-45.

Beser also explains that, if the unique identifier specifies a destination that can establish a secure tunnel such as the terminating end device or the destination of a VoIP request, the trusted-third-party network device will negotiate with the first and second network devices to establish the IP tunnel between those network

devices. Ex. 1007 at 9:6-11; *id.* 9:26-30, 11:9-44; Ex. 1005 at ¶¶ 324, 330. The secure tunnel described in Beser is a "secure communications service" because it enables the end devices to participate in a secure communications link (*i.e.*, a transmission path that restricts access to data, addresses, or other information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping). Ex. 1005 at ¶¶ 94-96.

Conversely, if a domain name in a request is recognized by the trusted-third-party network device but does not map to a device requiring negotiation of an IP tunnel, the trusted-third-party network device will simply return the IP address associated with the (non-secure) domain, as this is the known function of a DNS server on a public network. Ex. 1005 at ¶ 328; *see also* Ex. 1003 at 39:39-41. In this scenario, the first network device will simply process traffic from the originating device without attempting to establish a secure IP tunnel. Ex. 1007 at 8:21-50; Ex. 1005 at ¶ 317. Accordingly, Beser shows making a "*determination that the second network device is available for a secure communication service*" as specified in **claims 1 and 14**.

(3) "receiv[e/ing] . . . (1) an indication that the second network device is available for the secure communications service"

Both **claims 1 and 14** specify receiving, following the "interception" and "determination" discussed above, an "*indication that the second network device is*

available for the secure communications service." Beser explains that, if the trusted-third-party network device determines that a request contains a unique identifier for a destination that can establish a secure tunnel, it will negotiate with the first and second network devices to establish the IP tunnel. Ex. 1007 at 9:6-11; 9:26-30, 11:9-44; Ex. 1005 at ¶¶ 323-25, 330. Following negotiation of the IP tunnel, "[b]oth first 14 and second 16 network devices have obtained the private IP 58 addresses of the originating end of the tunneling association 24 that requested the initiation of the tunneling association and the terminating end of the tunneling association 26 that was associated with the unique identifier." Ex. 1007 at 14: 57-62. The originating end device also receives both private IP addresses. Ex. 1007 at 21:48-62.

The exchange of private IP addresses according to Beser's scheme results "in the establishment of a virtual tunneling association between the originating end and the terminating end of the tunneling association." Ex. 1007 at 8:15-18. By receiving both its own private IP address and the private address of the terminating end device, the originating end device ("*first network device*") receives an "indication" (*i.e.*, something that shows the probable presence or existence or nature of) that an IP tunnel is in operation and the terminating end device is able to communicate via the IP tunnel ("*that the second network device is available for the secure communications service*"). Ex. 1005 at ¶¶ 101, 341. Accordingly, Beser

shows receiving an indication that the second network device is available for a secure communications service as specified in **claims 1 and 14**.

(4) "receiv[e/ing] . . . (2) the requested network address of the second network device"

Both **claims 1 and 14** specify receiving the requested network address of the second network device. Beser explains "[t]he assignment of private network addresses to the ends of the tunneling association may also include transmitting the private network addresses to the network devices at the ends of the tunneling association where the private network addresses are stored on these end devices." Ex. 1007 at 21:48-52. The originating end device therefore receives the private IP address of the terminating end device. Ex. 1007 at 14:57-62, 21:48-52; Ex. 1005 at ¶ 340. The private IP address of the terminating end device is the "*the requested network address of the second network device*" because it was obtained based on an identifier associated with the second network device. Ex. 1007 at 7:62-8:20; 9:6-25; Ex. 1005 at ¶¶ 278, 310, 323-25. Accordingly, Beser shows receiving the requested network address as specified in **claims 1 and 14**.

(5) "receiv[e/ing] . . . (3) provisioning information for an encrypted communication link"

Both **claims 1 and 14** specify receiving "*provisioning information*" for an "*encrypted communication link*." First, as noted in § 0, Beser indicates that encryption is not necessarily used in its example showing streaming audio or video

data. In such an implementation, Beser would not provide provisioning information for an encrypted communication link, as the traffic being sent between the originating and terminating devices would not necessarily be encrypted. Providing such information, however, would have been an obvious variation of Beser in view of RFC 2401. Specifically, for the reasons provided above in § 0, a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § 0, *above.* Beser in view of RFC 2401 therefore would have rendered obvious establishing an "*encrypted communication link.*"

Second, Beser in combination with RFC 2401 would have rendered obvious receiving "*provisioning information*" for the encrypted communication link. Following the negotiation protocol in Beser, the originating end device receives (1) its own private IP address and (2) the private IP address assigned to the terminating end device. Ex. 1007 at 21:52-55; Ex. 1005 at ¶ 340. "[A]ny packet sent from the originating network device 24 to the first network device 14 may include the private network address of the originating and terminating ends of the tunneling association." Ex. 1007 at 21:55-58. The originating end device's own private IP address is therefore a type of "*provisioning information*" because it allows the

originating end device to communicate through a private IP tunnel where communications are encrypted according to IPsec (*i.e.*, information that enables communication in a virtual private network, where the virtual private network uses encryption). Ex. 1005 at ¶ 92.

RFC 2401 also describes providing "provisioning information." RFC 2401 explains that IPsec supports a variety of encryption key distribution techniques, including ones using a "KDC" (*i.e.*, a key distribution center), which is a trusted, centralized server for distributing keys (*e.g.*, a Kerberos server). Ex. 1008 at 7; Ex. 1005 at ¶¶ 136-140, 358-360. It would have been obvious to configure the trusted-third-party network device to play this role because it is a trusted and centralized intermediary. Ex. 1005 at ¶¶ 401-03. In this configuration, the trusted-third-party network device would generate and provide an encryption key to be used to encrypt the communications between the end devices according to IPsec. Ex. 1008 at 6-7, 9; Ex. 1005 at ¶¶ 401-03. Thus, it would have been obvious to configure the combined system to provide "*provisioning information*" in the form of an encryption key (*i.e.*, information that enables communication in a virtual private network, where the virtual private network uses encryption). Ex. 1005 at ¶¶ 401-03. Accordingly, Beser in view of RFC 2401 would have made obvious to the person of ordinary skill receiving provisioning information for an encrypted communication link as specified in **claims 1 and 14**.

d) "connect[ing] . . . over the encrypted communication link, using the received network address . . . and the provisioning information . . ."

Both **claims 1 and 14** specify a third step of connecting "*over the encrypted communication link*" to the second network device using the received network address and provisioning information. As noted in § 0, the Beser streaming video or audio example does not necessarily encrypt all the IP traffic sent over the secure tunnel. This distinction would have been an obvious variation of Beser when it is considered with RFC 2401.

First, Beser explains that its methods and systems result "in the establishment of a virtual tunneling association between the originating end and the terminating end of the tunneling association" (Ex. 1007 at 8:15-18), *i.e.*, between a "*first network device*" and a "*second network device*." A person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § 0, *above.* Beser in view of RFC 2401 therefore would have rendered obvious to "*connect to the second network device over the encrypted communication link.*"

Second, Beser shows that the connection between the originating and terminating end devices is established "using" the information received by the

originating end device as a result of the Beser scheme. Following the negotiation protocol in Beser, the originating end device receives (1) its own private IP address (*i.e.*, "*provisioning information for the encrypted communication link*") and (2) the private IP address assigned to the terminating end device (*i.e.*, "*the requested network address of the second network device*"). Ex. 1007 at 21:52-55; Ex. 1005 at ¶ 340. "[A]ny packet sent from the originating network device 24 to the first network device 14 may include the private network address of the originating and terminating ends of the tunneling association." Ex. 1007 at 21:55-58. Accordingly, Beser in view of RFC 2401 would have rendered obvious this third step specified in **claims 1 and 14**.

e) "communicat[e/ing] data . . . using the secure communications service via the encrypted communication link"

Both **claims 1 and 14** specify a last step of communicating data to the terminating end device "*using the secure communications service*" via "*the encrypted communication link.*" As noted in § 0, the Beser streaming video or audio example does not necessarily encrypt all the IP traffic sent over the secure tunnel. This distinction would have been an obvious variation for a person of ordinary skill considering Beser together with RFC 2401.

Initially, Beser shows that its scheme can be implemented using a wide variety of devices capable of engaging in secure communications such as

telephony and multimedia devices, routers, servers and modems. Ex. 1007 at 4:9-54; Ex. 1005 at ¶¶ 328-98. 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. 1007 at 1: 54-56, 4:55-5:2; Ex. 1005 at ¶¶ 282-83, 290-92, 384-86. Therefore, Beser shows "using" a "*secure communications service*" (*i.e.*, using "the functional configuration of a network device that enables it to participate in a secure communications link with another computer or device," where a "secure communications link" is "a transmission path that restricts access to data, addresses, or other information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping.").

Moreover, a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § 0, *above.* Therefore, Beser in view of RFC 2401 would have rendered obvious "using" the secure communications service "*via the encrypted communication link*" (*i.e.*, via "a transmission path that restricts access to data, addresses, or other information on the path at least by using encryption").

Accordingly, Beser in view of RFC 2401 would have rendered obvious this last step specified in **claims 1 and 14**.

f) "the first network device being a device at which a user uses the secure communications service to access the encrypted communication link"

Finally, Beser in view of RFC 2401, would have rendered obvious a method for establishing a secure communications service, and a network device configured to perform that method, wherein the network device is "*a device at which a user uses the secure communications service to access the encrypted communication link*" as specified in **claims 1 and 14**. As noted in § 0, the Beser streaming video or audio example does not necessarily encrypt all the IP traffic sent over the secure tunnel. This distinction would have been an obvious variation of Beser when it is considered with RFC 2401.

Beser explains that the originating and terminating end devices can be telephony devices (including VoIP devices or personal computers running facsimile or audio applications) or multimedia devices (such as Web-TV sets and decoders, interactive video game players and personal computers running multimedia applications). Ex. 1007 at 4:43-52; Ex. 1005 at ¶¶ 286-91. These are all devices that can be used directly by an user to establish and access an encrypted IP tunnel according to the combined teachings of Beser and RFC 2401. Ex. 1007 at 8:15-20; § 0, *above.* In other words, these are all types of devices that allow a

user to use "the functional configuration of a network device that enables it to participate in a secure communications link with another computer or device" (*i.e.*, "*secure communications service*") to access "a transmission path that restricts access to data, addresses, or other information on the path at least by using encryption" (*i.e.*, "*encrypted communication link*"). Ex. 1005 at ¶¶ 91, 96. Accordingly, Beser in view of RFC 2401 would have made obvious this limitation in **claims 1 and 14**.

g) Additional System Elements of Claim 1

Claim 1 specifies a network device comprising (1) a "storage device" storing an application program for a secure communications service; and (2) at least one "processor" configured to execute the application program. Beser explains that the "operating environment for network devices and modified routers of the present invention include[s] a processing system with at least one high speed Central Processing Unit ("CPU") and a memory." Ex. 1007 at 5:15-18. Beser also explains that its systems are implemented using programmed computers and other programmable devices that have processing elements and storage media containing code that configures how those devices function. Ex. 1005 at ¶ 293. For example, Beser explains that the originating end device can be a telephony device (*e.g.*, a VoIP device or a personal computer running facsimile or audio applications) or a multimedia device (*e.g.*, a WebTV set, interactive video game players or personal

computers running multimedia applications). Ex. 1007 at 4:43-52. It was known in February 2000 that personal computers include processors and storage devices. Ex. 1005 at ¶ 293. Telephony devices and multimedia devices such as those described in Beser include memory and processing elements. *Id*. Beser thus shows an originating end device ("*network device*") comprising "*a storage device*" and "*at least one processor*" as specified in the preamble of **claim 1**. Further, Beser explains that its IP tunneling scheme is compatible with end devices running "multimedia applications" or "facsimile or audio applications." Ex. 1007 at 4: 47-52; Ex. 1005 at ¶¶ 289-89. Beser therefore also shows "*an application program for a secure communications service*" as specified in the preamble of **claim 1**.

3. Claims 2 and 15 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 2 and 15 depend, respectively. *See* § IV.C.2, *above*. Claims 2 and 15 further specify that the secure communications service includes an "*audio-video conferencing service*" and the at least one processor is configured to communicate *"at least one of encrypted video data and audio data*" with the second network device via the encrypted communication link using the secure communications service. Beser explains that a variety of types of data can be transmitted through its IP tunnel including VoIP traffic, "multimedia" content (*e.g.*, video, audio), video conference traffic, or content for web pages (*e.g.*,

delivered to WebTV devices or decoders or personal computers). Ex. 1007 at 4:43-54, 6:24-57, 9:64-10:2; Ex. 1005 at ¶ 312. Beser thus shows a method and a network device wherein the secure communications service includes "*an audio-video conferencing service*" and at least one processor is configured to communicate "*video data and audio data*" as specified in **claims 2 and 15**.

Further, as discussed above, a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § 0, *above*. Beser in combination with RFC 2401 therefore would have made it obvious that the video and audio data are encrypted and communicated "*via the encrypted communication link using the secure communications service*." Accordingly, Beser in view of RFC 2401 would have rendered obvious **claims 2 and 15**.

4. Claims 3 and 16 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 3 and 16 depend. *See* § IV.C.2, *above*. Claims 3 and 16 further specify that the secure communications service includes a "*telephony service*." Beser explains that the originating and terminating end devices can be "telephony devices" including "VoIP devices (portable or stationary) or personal computers

running facsimile or audio applications." Ex. 1007 at 4:43-52, Figs. 1 and 17. Beser in view of RFC 2401 would have also rendered obvious **claims 3 and 16**.

5. Claims 6 and 19 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 6 and 19 depend. *See* § IV.C.2, *above*. Claims 6 and 19 further specify that the network device is a "*mobile device*." Beser states that the originating and terminating end devices can be "portable" devices. Ex. 1007 at 4:43-52; Ex. 1005 at ¶¶ 287-90. Beser in view of RFC 2401 therefore would have also rendered obvious **claims 6 and 19**.

6. Claims 4, 5, 17 and 18 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1, 3 and 14, from which claims 4, 5, 17 and 18 depend. *See* §§ IV.C.2, IV.C.4, *above*. Claims 4 and 17 further specify that the telephony service uses "*modulation*." Claims 5 and 18 further specify that the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

Beser explains that the data that can be transmitted through an IP tunnel can represent VoIP traffic or video conference traffic, and shows several examples of devices that can be used to transmit such data. Ex. 1007 at 4:19-54; Ex. 1005 at ¶¶ 286-89, 294, 297, 312. For example, Beser explains that the first and second

network device each can be a cable modem. Ex. 1007 at 4: 30-42. It was well known before February of 2000 that data transmitted via a cable modem inherently will be modulated, and that cable modems used various types of modulation, including FDM and TDM. Ex. 1005 at ¶ 297.

Beser also explains that end devices can include portable VoIP devices such as mobile phones, and that data can be sent to and from such a device using data transmission standards that were developed by the Wireless Application Protocol ("WAP") Forum. Ex. 1007 at 43-63; Ex. 1005 at ¶¶ 290-92. In was known in February 2000 that data transmitted to a mobile device using WAP could be transmitted over a cellular network, such as a GSM network (which employed TDM) or a CDMA network. Ex. 1005 at ¶¶ 80, 290-92. Accordingly, Beser in view of RFC 2401 would have also rendered obvious **claims 4, 5, 17 and 18**.

7. Claims 7 and 20 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 7 and 20 depend. *See* § IV.C.2, *above*. Claims 7 and 20 further specify "*wherein the identifier associated with the second network device is a domain name*." To establish an IP tunnel according to Beser, the originating end device sends a request containing a unique identifier specifying a destination (*i.e.*, a terminating end device). Ex. 1007 at 7:62-8:3; Ex. 1005 at ¶¶ 316, 318-19. The unique identifier can be a domain name. Ex. 1007 at 10:37-41, 10:55-11:5. Beser

in view of RFC 2401 therefore also would have rendered obvious **claims 7 and 20**.

8. Claim 8 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claim 1 from which claim 8 depends. *See* § IV.C.2, *above*. Claim 8 further specifies "*wherein the encrypted communication link is part of a virtual private network communication link.*" Beser shows that the trusted-third-party device, along with the first and second network devices, are used to establish secure IP tunnels. Ex. 1007 at 7:62-8:20. The trusted-third-party network device is connected to a public communication network. Ex. 1007 at 8:3-12, Fig. 1. Beser shows that its IP tunnels allow end devices to directly communicate over a secure and anonymous channel. Ex. 1007 at 8:15-20, 12:13-16, 22:2-8; Ex. 1005 at ¶ 344.

As discussed above, a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § 0, *above*. Beser in view of RFC 2401 thus shows an encrypted communication link that is part of a "virtual private network communication link" (*i.e.*, a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to,

one or more of authentication, encryption, or address hopping). Ex. 1005 at ¶ 105. Beser in view of RFC 2401 therefore would have rendered obvious **claim 8**.

9. Claims 10 and 22 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claim 1 and 14, from which claims 10 and 22 depend, respectively. *See* § IV.C.2, *above*. Claims 10 and 22 further specify "*wherein the indication that the second network device is available for the secure communications service is a function of the result of a domain name lookup*." Beser teaches that the trusted-third-party network device receives a requests containing a unique identifier and checks its internal database ("*a domain lookup*") to determine whether the unique identifier specifies a destination that can establish a secure tunnel ("*the second network device is available for the secure communications service*"). Ex. 1007 at 11:30-36, 11:45-58; Ex. 1005 at ¶¶ 322-325. If so, the trusted-third-party network device will negotiate with the first and second network devices to establish the IP tunnel between those network devices. Ex. 1007 at 9:6-11; *id*. 9:26-30, 11:9-44; Ex. 1005 at ¶ 330. Following negotiation of the IP tunnel, the originating end device receives both its own private IP address and the private IP address assigned to the terminating end device. Ex. 1007 at 21:48-62. The originating end device therefore receives an "indication" (*i.e.,* something that shows the probable presence or existence or nature of) that the second network device is available for the secure

communications service. Ex. 1005 at ¶ 341.

Conversely, if the unique identifier in a request is not recognized by the trusted-third-party network device or does not map to a device requiring negotiation of an IP tunnel, the trusted-third-party network device will not negotiate private IP addresses. Ex. 1005 at ¶¶ 326-329; *see also* Ex. 1003 at 39:36-38. The "indication" in Beser is therefore a function of the outcome of the trusted-third-party network device's lookup in its internal database ("*a function of the result of a domain name lookup*"). Thus, Beser in view of RFC 2401 would have also rendered obvious **claims 10 and 22**.

10. Claims 11 and 23 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 11 and 23 depend, respectively. *See* § IV.C.2, *above*. Claims 11 and 23 further specify that the encrypted communication link is an "*end-to-end link extending from the network device to the second network device.*" As discussed above, a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices. *See* § 0, *above.* Accordingly, a person of ordinary skill considering the IP tunneling scheme of Beser in view of RFC 2401 would have found it obvious to

encrypt communications end-to-end. Ex. 1005 at ¶ 399. Thus, Beser in view of RFC 2401 would have rendered obvious **claims 11 and 23**.

11. Claims 12 and 24 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 12 and 24 depend, respectively. *See* § IV.C.2, *above*. Claims 12 and 24 further specify "*wherein the intercept[ion/ing] the DNS request consists of receiving the DNS request to determine that the second network device is available for the secure communications service.*" Beser does not explicitly describe what would happen if the unique identifier was not listed in the trusted-third-party network device's database of registered identifiers. Configuring the trusted-third-party network device to handle such an error condition would have been a simple engineering design choice, which would have been routinely made by a person of ordinary skill in the art. Ex. 1005 at ¶ 326. The tunneling application on the trusted-third-party network device could (i) do nothing, (ii) return an error code, or (iii) pass the unique identifier to a conventional domain name server or directory service for resolution. *Id.* Alternatively, if a domain name in a request is recognized by the trusted-third-party network device but does not map to a device requiring negotiation of an IP tunnel, the trusted-third-party network device will simply return the IP address associated with the (non-secure) domain, as this is the known function of a DNS server on a public network. Ex.

1005 at ¶ 328; *see also* Ex. 1003 at 39:39-41.

In contrast, if the trusted-third-party network device determines that the unique identifier in a request specifies a destination that can establish a secure tunnel, it will negotiate with the first and second network devices to establish the IP tunnel between those network devices. Ex. 1007 at 9:6-11, 9:26-30, 11:9-44; Ex. 1005 at ¶ 330. Consequently, when methods shown in Beser are performed, the trusted-third-party network device will "receive" a request and "determine" whether the unique identifier specifies a terminating end device ("*second network device*") that accepts secure communications ("*is available for the secure communications service*") by checking its internal database. Ex. 1007 at 11:30-36, 11:45-58; Ex. 1005 at ¶¶ 323-25. This is the same type of "determination" disclosed in the '009 patent. *See* Ex. 1003 at 40:39-45; *see also* § IV.C.2.c)(2), *above*. Therefore, Beser in view of RFC 2401 would have rendered obvious **claims 12 and 24**.

12. Claims 13 and 25 Would Have Been Obvious

Beser in view of RFC 2401 would have rendered obvious claims 1 and 14, from which claims 13 and 25 depend, respectively. *See* § IV.C.2, *above*. Claims 13 and 25 further specify "*wherein the intercepting the request occurs within another device that is separate from the network device.*" Beser explains that an originating end device sends a request to initiate a tunneling association with a

terminating end device. Ex. 1007 at 7:64-8:1; Ex. 1005 at ¶ 316. The request will be received not by the terminating end device, but by a first network device, which evaluates all of the data packets it receives. Ex. 1007 at 8:21-47; Ex. 1005 at ¶ 317. Beser also explains that, if the first network device determines that a request to initiate an IP tunnel with another device has been made, it will forward the request to the trusted-third-party network device ("*another device that is separate from the network device*"). Ex. 1007 at 22:8-22; Ex. 1005 at ¶ 322. Therefore, Beser in view of RFC 2401 would have also rendered obvious **claims 13 and 25**.

D. No Secondary Considerations Exist

As described above, Beser in view of RFC 2401 teaches systems and processes that render *prima facie* obvious each of the challenged claims of the '009 patent. No secondary indicia of non-obviousness exist having a nexus to the putative "invention" of the '009 patent contrary to that conclusion. Petitioner reserves its right to respond to any assertion of secondary indicia of non-obviousness advanced by Patent Owner.

V. Conclusion

Petitioner respectfully submits that the evidence presented in this Petition establishes a reasonable likelihood that Petitioner will prevail in establishing the challenged claims are unpatentable, and requests that Trial be instituted.

Dated: March 2, 2015

Respectfully Submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005
jkushan@sidley.com
(202) 736-8914
Attorney for Petitioner

PETITION FOR *INTER PARTES* REVIEW

OF U.S. PATENT NO. 8,850,009

Attachment A:

Proof of Service of Petition

CERTIFICATE OF SERVICE

I hereby certify that on this 2nd day of March, 2015, copies of this Petition for *Inter Partes* Review, Attachments and Exhibits have been served in its entirety by Federal Express on the following counsel of record for Patent Owner:

VirnetX, Inc.
P.O. Box 439
308 Dorla Court
Zephyr Cove, Nevada 89448

Joseph E. Palys
Paul Hastings LLP
875 15th Street, NW
Washington, D.C. 20005

Toby H. Kusmer
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775

Naveen Modi
Paul Hastings LLP
875 15th Street, NW
Washington, D.C. 20005

Toby H. Kusmer
McDermott Will & Emery LLP
The McDermott Building
500 North Capitol Street, N.W.
Washington, D.C. 20001

Jason E. Stach
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
3500 SunTrust Plaza
303 Peachtree Street, NE
Atlanta, GA 30308-3263

Dated: March 2, 2015

Respectfully submitted,

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

PETITION FOR *INTER PARTES* REVIEW

OF U.S. PATENT NO. 8,850,009

Attachment B:

Exhibit List

Exhibit #	Reference Name
1001	U.S. Patent 8,868,705
1002	U.S. Patent 8,868,705 File History
1003	U.S. Patent 8,850,009
1004	U.S. Patent 8,850,009 File History
1005	Declaration of Roberto Tomassia
1006	Curriculum Vitae of RobertoTomassia
1007	U.S. Patent 6,496,867 to Beser
1008	Kent, S., et al., RFC 2401, "Security Architecture for the Internet Protocol" (November 1998)
1009	Aventail Connect v3.01/v2.51 Administrator's Guide (1996-1999)
1010	Aventail Connect v3.01/v2.51 User's Guide (1996-1999)
1011	Aventail ExtraNet Center v3.0 Administrator's Guide (NT and UNIX)
1012	U.S. Patent 5,237,566 to Brand
1013	Handley, M., et al., RFC 2543, SIP: Session Initiation Protocol (March 1999)
1014	RFC 793, DARPA Internet Program Protocol Specification (September 1991)
1015	U.S. Patent Number 6,430,176 to Christie
1016	U.S. Patent Number 6,930,998 to Sylvain
1017	Patent Owner Preliminary Response, IPR2014-00237, Paper 12 (March 6, 2014)
1018	Leech, M., et al., RFC 1928, SOCKS Protocol Version 5 (March 1996)
1019	Microsoft Computer Dictionary (4th Ed.)
1020	U.S. Patent Number 6,408,336 to Schneider
1021	U.S. Patent Number 5,633,934 to Hember
1022	Declaration of James Chester, Reexamination 95/001,697

Exhibit #	Reference Name
1023	Declaration of Chris Hopen, Reexamination 95/001,697
1024	U.S. Patent 6,557,037 to Provino
1025	Gunter, M., "Virtual Private Networks Over the Internet" (1998)
1026	Patent Owner Preliminary Response, IPR2014-00404, Paper 9 (May 19, 2014)
1027	von Sommering, S., Space Multiplexed-Electrochemical Telegraph
1028	Licklider, J.C.R., Memorandum for Members and Affiliates of the Intergalactic Computer Network (December 11, 2001)
1029	BBN Report No. 1822, Interface Message Processor (January 1976)
1030	Koblas, D., et al., "SOCKS-Usenix Unix Security Symposium III"
1031	Windows NT for Dummies
1032	Mockapetris, P., RFC 882, "Domain Names – Concepts and Facilities" (November 1983)
1033	Mockapetris, P., RFC 883, "Domain Names – Implementation and Specification" (November 1983)
1034	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities" (November 1987)
1035	Mockapetris, P. RFC 1035, "Domain Names – Implemenation and Specification" (November 1987)
1036	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3" (October 1996)
1037	Rosen, E., et al., RFC 2547, "BGP/MPLS VPNs" (March 1999)
1038	W3C and WAP Forum Establish Formal Liason Relationship (December 8, 1999)
1039	Wireless Application Protocol (WAP) Architecture Specification (April 30, 1998)
1040	H.323 ITU-T Recommendation (February, 1998)
1041	Kiuchi, T., et al., "C-HTTP – The Development of a Secure, Closed HTTP-Based Network on the Internet" (IEEE 1996) LOC Stamped
1042	VirnetX's Opening Claim Construction brief, VirnetX, Inc. v. Cicso Systems, Inc., et al., Civil Action No. 6:10-cv-417 (EDTX) (November 4, 20111)

Exhibit #	Reference Name
1043	Declaration of Michael Fratto, Reexamination 95/001,682
1044	U.S. Patent 5,898,830 to Wesinger
1045	Steiner, J., et al., "Kerberos: An Authentication Service for Open Network Systems" (January 12, 1988)
1046	Harkins, D., et al., RFC 2409, "The Internet Key Exchange (IKE) (November 1998)
1047	Maughan, D., et al., "Internet Security Association and Key Management Protocol (ISAKMP)" (November 1998)
1048	Data-Over-Cable Interface Specifications (DOCIS), Radio Frequency Interface Specification (March 26, 1997)