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. 8,504,697
Issued: August 6, 2013
Filed: December 28, 2011
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. IPR2014-00237

PETITION FOR INTER PARTES REVIEW

TABLE OF CONTENTS

I. COMPLIANCE WITH REQUIREMENTS FOR A PETITION FOR INTER PARTES REVIEW 1
A. Certification the ’697 Patent May Be Contested by Petitioner 1
B. Fee for Inter Partes Review (§ 42.15(a)) 2
C. Mandatory Notices (37 CFR § 42.8(b)) 2
1. Real Party in Interest (§ 42.8(b)(1)) 2
2. Other Proceedings (§ 42.8(b)(2)) 2
3. Designation of Lead and Backup Counsel 2
4. Service Information (§ 42.8(b)(4)) 2
D. Proof of Service (§§ 42.6(e) and 42.105(a)) 2
II. IDENTIFICATION OF CLAIMS BEING CHALLENGED (§ 42.104(B)) 2
III. RELEVANT INFORMATION CONCERNING THE CONTESTED PATENT 3
A. Effective Filing Date and Prosecution History of the ’697 patent 3
B. Person of Ordinary Skill in the Art 5
C. Construction of Terms Used in the Claims 6
1. Domain Name (Claims 1-11, 14-25, and 28-30) 6
2. Secure Communication Link (Claims 1-11, 14-25, and 28-30) 7
3. Secure Communications Service (Claims 1-11, 14-25, 28-30) 10
4. Intercepting . . . a request (Claims 1-11, 14-25, and 28-30) 12
5. Modulation (Claims 6-7 and 20-21) 15
IV. PRECISE REASONS FOR RELIEF REQUESTED 16
A. Claims 1-11, 14-25, and 28-30 Are Anticipated by Beser 16
1. Beser Anticipates Claims 1 and 16 16
2. Beser Anticipates Claim 2 and 24 23
3. Beser Anticipates Claim 3 and 17 24

4. Beser Anticipates Claim 4 and 18 25
5. Beser Anticipates Claims 5, 6, 7, 19, 20, and 21 26
6. Beser Anticipates Claim 8, 9, 22 and 23 27
7. Beser Anticipates Claim 10 and 29 28
8. Beser Anticipates Claim 11 and 25 30
9. Beser Anticipates Claim 14 and 28 30
10. Beser Anticipates Claim 15 and 30 32

B. Beser In View of RFC 2401 Renders Obvious Claims 1-11, 14-25, and 28-30 33
1. Claims 2 and 24 Would Have Been Obvious 33
2. Dependent Claims 3 and 17 Would Have Been Obvious 37
3. Claims 1, 16, 4-11, 16, 18-23, 25, and 28-30 Would Have Been Obvious 38

C. Claims 1-11, 14-25, and 28-30 Are Anticipated by RFC 2543 39
1. RFC 2543 Anticipates Claims 1 and 16 39
2. RFC 2543 Anticipates Claim 2 and 24 48
3. RFC 2543 Anticipates Claim 3 and 17 49
4. RFC 2543 Anticipates Claim 4 and 18 50
5. RFC 2543 Anticipates Claim 5, 6, 7, 19, 20, and 21 50
6. RFC 2543 Anticipates Claim 8, 9, 22, and 23 52
7. RFC 2543 Anticipates Claim 10 and 29 53
8. RFC 2543 Anticipates Claim 11 and 25 54
9. RFC 2543 Anticipates Claim 14 and 28 54
10. RFC 2543 Anticipates Claim 15 and 30 56

D. RFC 2543 In View of RFC 1889, RFC 2327 Renders Obvious Claims 1-11, 14-25, and 28-30 56
1. Independent Claims 1 and 16 Would Have Been Obvious 56
2. Dependent Claims 2-11, 14-15, 17-25, and 28-30 Would Have Been Obvious 57

E. RFC 2543 In View of Mobility Support Using SIP Renders Obvious Claims 8-9 and 22-23 58

V. CONCLUSION 60

Attachment A. Proof of Service of the Petition
Attachment B. List of Evidence and Exhibits Relied Upon in Petition

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

A. Certification the '697 Patent May Be Contested by Petitioner

Petitioner certifies that U.S. Patent No. 8,504,697 (the '697 patent) (Ex. 1001) is available for *inter partes* review. Petitioner certifies that it is not barred or estopped from requesting *inter partes* review of the claims of the '697 patent on the grounds identified in this Petition. Neither Petitioner, nor any party in privity with Petitioner, has filed a civil action challenging the validity of any claim of the '697 patent. The '697 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 filed within one year of the date of service of a complaint alleging infringement of a patent. On **August 5, 2013**, VirnetX filed a complaint in the Eastern District of Texas asserting the '697 patent in case No. 6:13-cv-00581. The case was dismissed without prejudice. On **August 27, 2013**, VirnetX amended its complaint in the 6:12:cv-00855 proceeding to add the '697 patent. Because the date of this petition is less than one year from **August 27, 2013**, 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 '697 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 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))

The '697 patent is not subject to any other proceedings. The '697 patent is also the subject of IPR2014-00238 being filed concurrently by Petitioner.

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 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 **1-11, 14-25, and 28-30** of the '697 patent are unpatentable as being anticipated under 35 U.S.C. § 102(a) & (e), and/or for being obvious over the prior art under 35 U.S.C. § 103. Specifically:

(i) Claims **1-11, 14-25, and 28-30** are anticipated under § 102(e) by U.S. Patent No. 6,496,867 to Beser ("Beser") (Ex. 1009);

(ii) Claims **1-11, 14-25, and 28-30** are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010);

(iii) Claims **1-11, 14-25, and 28-30** are obvious under § 103 based on Beser (Ex. 1009) in view of RFC 2401 (Ex. 1010) and the knowledge of a person of ordinary skill in the art;

(iv) Claims **1-11, 14-25, and 28-30** are anticipated under § 102(a) by RFC 2453 (Ex. 1012);

(v) Claims **1-11, 14-25, and 28-30** are obvious under § 103 based on RFC 2453 (Ex. 1012) in view of RFC 1889 (Ex. 1013) and RFC 2327 (Ex. 1014).

(vi) Claims **8-9 and 22-23** are obvious under § 103 based on RFC 2453 (Ex. 1012) in view of Mobility Support Using SIP (Ex. 1015).

Petitioner's proposed construction of the contested 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 '697 patent

The '697 patent issued from U.S. Ser. No. 13/339,257. The '257 application claims the benefit as a continuation of the following applications: (i) 13/049,552

(issued as U.S. Patent No. 8,572,247); 11/840,560 (issued as U.S. Patent No. 7,921,211); 10/714,849 (issued as U.S. Patent No. 7,418,504); and 09/558,210. It also is designated a **continuation-in-part** of 09/504,783, filed on February 15, 2000, 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 16 of the '697 patent are independent claims. Claims 2-11 and 14-15 depend directly or indirectly from **claim 1**, and claims 17-25 and 28-30 depend directly or indirectly from **claim 16**. Claims 2-11, 14-15, 17-25, and 28-30 cannot enjoy an effective filing date earlier than that of claims 1 and 16, respectively, from which they depend (*i.e.*, no earlier than **February of 2000**).

Claims 1 and 16 of the '697 patent rely on information found only in the '783 application. For example, claim 1 of the '697 patent specifies "intercepting . . . a request to look up an internet protocol (IP) address . . . based on a **domain name** . . . ." Claim 16 specifies "[a] system . . . including one or more servers configured to intercept . . . a request to look up an internet protocol (IP) address . . . based on a **domain name** . . . ." No application filed prior to the '783 application even mentions the term "domain name," much less provides a written description of systems or processes corresponding to the '697 patent claims. In proceedings involving the related '135, '151, '211 and '504 patents, Patent Owner has not

disputed that claims reciting a "domain name" 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, -00376, -00377, -00378, -00393, -00394, -00397, and -00398. 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. Also, while claims 1 and 16 recite a "**secure communications service**," there is no mention, whether explicit or implicit, of this term anywhere in the disclosure of the '697 patent, nor in any application filed prior to the '783 application. Thus, the effective filing date of claims 1-11, 14-25, and 28-30 of the '697 patent is not earlier than **February 15, 2000**.

B. Person of Ordinary Skill in the Art

A person of ordinary skill in the art in the field of the '697 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. 1003 ¶ 63.

C. Construction of Terms Used in the Claims

In this proceeding, claims must be given their broadest reasonable construction in light of the specification. 37 CFR § 42.100(b). The broadest reasonable construction should take account of Patent Owner's contentions as to what the claims literally encompass and constructions Patent Owner has advanced in litigation. The '697 patent shares a common disclosure and uses several of the same terms as the '135, '151, '504 and '211 patents, in respect of 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 district court litigation, which employs a different claim construction standard.

1. Domain Name (Claims 1-11, 14-25, and 28-30)

The '697 patent does not define the term "**domain name**." A person of ordinary skill would understand that the ordinary meaning of a "domain name" is a

hierarchical sequence of words in decreasing order of specificity that corresponds to a numerical IP address. Ex. 1003 at ¶¶ 89-91; *see generally* ¶¶ 86-94. Patent Owner, however, has asserted a "domain name" is simply "a name corresponding to an IP address." Ex. 1046 at 14-15. The broadest reasonable construction of "domain name" should encompass Patent Owner's contention that it can be "a name corresponding to an IP address." *See* Ex. 1003 at ¶¶ 199-201.

2. Secure Communication Link (Claims 1-11, 14-25, and 28-30)

The broadest reasonable construction of the phrase "secure communication link" can include communications over a virtual private network (VPN), would encompass communications that are encrypted or not encrypted, and would encompass direct communications between computers involved in the secure communications link that are transported via intermediary computers or devices.

First, the '697 patent explains a "secure communication link" is "a virtual private communication link over the computer network." Ex. 1001 at 6:63-65. A "secure communication link" therefore must encompass virtual private networks. Ex. 1003 at ¶¶ 202-210; *see* Ex. 1001 at claims 3 and 17. It also suggests that a "secure communication link" is one that permits computers to privately communicate with each other over a public network – a communication link would be "secure" if it protects the anonymity of the computers involved in the communications. *See, e.g.*, Ex. 1001 at 39:49-58.

Second, dependent claims 2 and 24 of the '697 patent specify that data being sent over a "secure communication link" must be encrypted. *See, e.g.*, Ex. 1001 at claim 2 ("…wherein at least one of the video data and the audio data is encrypted over the secure communication link."). By contrast, claims 1 and 16 specify only that the "secure communication link [be used] to communicate at least one of video data and audio data" between the two network devices. Under the doctrine of claim differentiation, the broadest reasonable construction of a "secure communication link" means that data being sent over the secure communication link may or may not be encrypted.[1]

[1] In proceedings involving the '135,'504, and '211 patents, Patent Owner has contended a VPN requires network traffic to be encrypted, a contention that is inconsistent with the common disclosure of the '135, '504, '211, and '697 patents. *See, e.g.*, Ex. 1001 at 1:57-59 ("Data security is usually tackled using some form of data encryption"); 2:44-54 (referring to technique that does not use encryption to protect the anonymity of the VPN); *see also* Ex. 1003 ¶¶ 200-208. In addition, while the '697 patent shows use of TARP routers that do encrypt all network traffic (Ex. 1001 at 3:16-3:46), it does not state that TARP routers are required for the disclosed DNS-based VPN scheme. *See, e.g.*, Ex. 1001 at 40:10-14 ("The VPN is preferably implemented using the IP address "hopping" features of the basic

(Footnote continued)

Third, based on Patent Owner's representations in other proceedings involving related patents, the broadest reasonable construction of a "secure communication link" would encompass direct communications between computers that are transmitted via intermediary computers and devices. For example, one district court has found, based on the disclosure of the common disclosure of the '697 and '135 patents, 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. 1049 at 8 (FN2).

The broadest reasonable construction of "secure communication link" thus encompasses "a communication link in which computers privately and directly communicate with each other on insecure paths between the computers where the

---

invention described above…" (emphasis added)). The '697 patent also does not show any encryption steps in the DNS-related VPN scheme it describes. See Ex. 1001 at 39:28-42:16. Also, in February of 2000, it was understood that a VPN could be established without encryption (e.g., by using "obfuscation" techniques to ensure the security and anonymity of the network traffic over a public network). *See* Ex. 1003 ¶ 208; Ex. 1073 at 2.

communication is both secure and anonymous, and where the data transferred may or may not be encrypted." [2] *See* Ex. 1003 at ¶¶ 202-210.

3. Secure Communications Service (Claims 1-11, 14-25, 28-30)

The '697 patent does not expressly define the term "**secure communications service**." Instead, its manner of use of this phrase in the two places in the disclosure where it appears (excluding the abstract) indicates that a "secure communications service" is simply referring to the capacity of two computers to participate in secure communications link. For example, the '697 patent states:

> The method comprises: receiving, from the first network device, a request to look up a network address of the second network device based on an identifier associated with the second network device; determining, in response to the request, whether the second network device **is available for a secure communications service**; and initiating a secure communication link between the first network device and the second network device based on a determination that

[2] In the grandparent of the present patent (*i.e.*, the '504 patent), Patent Owner unequivocally disclaimed secure communication links that did not employ encryption. *See* Ex. 1056 at 25. This disclaimer limits the scope of the claims, including the '697 claims, that use this term in district court proceedings, which do not employ the broadest reasonable construction used in these proceedings.

> the second network device **is available for the secure communications service**; wherein **the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device**.

Ex. 1001 at 8:9-24; *see also id.* at 40:4-9 ("a specialized DNS server traps DNS requests and, if the request is from a special type of user (*e.g.*, one for which **secure communication services** are defined), the server . . . automatically sets up a virtual private network between the target node and the user").

The capacity of two computers to participate in a secure communications link means that the computers must be configured to enable them to handle the communications that are required for that secure communications link. The term "service" is often used by persons of ordinary skill in the art to refer to the configuration of a computer that provides the computer with some functional capability. Ex. 1003 at ¶ 214. The '697 patent, however, provides no description of any software or logic that confers on computers the ability to participate in a secure communications link.

The broadest reasonable construction of the term "secure communications service" thus refers to the functional configuration of a computer that enables it to participate in a secure communications link with another computer.

4. Intercepting . . . a request (Claims 1-11, 14-25, and 28-30)

The broadest reasonable construction of "**intercepting … a request**" would include a proxy computer or device receiving and acting on a request sent by a first computer that was intended for another computer.[3] This interpretation is consistent with the use of the term "intercepting" in the independent and dependent claims, in the specification, and in its conventional meaning.

The '697 patent does not expressly define the phrase "intercepting ... a request." Also, as used in the claims, the term "intercepting" refers to a single event – receiving a particular type of request (*i.e.*, a request to look up an IP address of a second network device based on a domain name of that device). Dependent claims 10 and 29 also specify that "intercepting" must necessarily encompass "receiving" a request. For example, claim 10 specifies the step of "intercepting … the request" in claim 1 consists of "**receiving** the request to determine whether the second network device is available for the secure communications service." Similarly, claim 29 provides that the servers of claim 16 are configured to "intercept the request **by receiving** the request to determine

[3] Claim 1 uses the phrase "intercepting … a request" while claim 16 uses the term "intercept … a request." There is no substantive distinction apparent from the tense of the word "intercept." *See* Ex. 1003 at ¶ 218.

whether the second network device is available for the secure communications service."

The specification uses the term "intercepting" in a consistent manner. For example, the specification describes a process where a proxy server will "intercept" a request instead of a DNS server, and then act on the request. *See, e.g.*, Ex. 1001 at 40:31-33 ("According to one embodiment, **DNS proxy 2610 intercepts** all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested." (emphasis added)). The specification also shows the network configuration will send all DNS requests to the DNS proxy server – it is pre-configured to route the traffic to a known destination (*i.e.*, the DNS proxy server) instead of a DNS server, which ordinarily would receive and resolve the domain name in the request. *Id.* This use of "intercept" in the specification as meaning receipt of a message by a proxy server instead of the intended destination is consistent with the ordinary meaning of the term "intercept" – which is to receive a message intended for another. *See* Ex. 1079 at 3 ("…to obtain covertly (a message, etc. intended for another)…")

The prosecution history of the '697 patent is relevant to what the claims in their broadest reasonable interpretation encompass. Claims 1 and 16 originally recited "receiving … a request to look up a network address." These claims were rejected as being obvious over Wesinger (Ex. 1008). Rather than arguing the

claims were not obvious, Patent Owner amended claims 1 and 16 to: (i) recite "intercepting … a request" instead of "receiving … a request"; and (ii) changing "network address" to "Internet Protocol (IP) address." Patent Owner also added new claims 10 and 29, which depend from claims 1 and 16, respectively. Following the amendments, the Examiner found the claims allowable, explaining in the Notice of Allowance that the prior art "may not clearly disclose the feature of 'intercepting a request to look up an IP address based on a domain name of a secure web site (i.e., the second network device) and determining whether or not to establish a secure connection.'" Ex. 1002 (FH) at 1034 (emphasis in original).

The file history demonstrates that the Examiner failed to appreciate the impact of Patent Owner's newly added dependent claims 10 and 29; namely, that they caused the broadest reasonable interpretation of independent claims 1 and 16 to necessarily encompass "receiving" a request.[4] This is notable because the claims employing the "receiving … the request" language had previously been found unpatentable over Wesinger by the Examiner, and that the Patent Owner

[4] The Examiner also appears to have used the incorrect legal standard (*i.e.*, anticipation) to assess obviousness when he found the claims patentable (*i.e.*, because the prior art "may not clearly disclose the feature of 'intercepting a request …'"). Ex. 1002 (FH) at 1034.

acquiesced to that finding by amending the claims, rather than arguing that the "receiving" claims were not obvious. Given that the claims in their broadest reasonable construction must necessarily encompass "receiving … a request" pursuant to claims 10 and 29, they are clearly unpatentable over Wesinger, and Patent Owner cannot now dispute otherwise, given its acquiescence to this finding of unpatentability by the Examiner.[5]

5. Modulation (Claims 6-7 and 20-21)

The '697 patent does not define the term "**modulation**." A person of ordinary skill would understand that the term "modulation" refers to the process of encoding data for transmission over a physical medium by varying or "modulating" a carrier signal. Ex. 1003 at ¶¶ 235-239. Any data transmitted via a

[5] *See, e.g.*, *Sciele Pharma Inc. v. Lupin Ltd*., 684 F.3d 1253, 1261 (Fed. Cir. 2012) (Federal Circuit vacated grant of a preliminary injunction, finding a "substantial question of invalidity" was raised in part by the Examiner's overt error in the prosecution history, and that "[o]ther than recognizing that the prosecution history was 'puzzling,' the district court did not discuss the prosecution history, which demonstrates that the examiner concluded that the claims with an upper Tmax limit of 7.5 were not patentable in view of Cheng and that the applicant acquiesced in that conclusion and cancelled those claims.").

modem (*i.e.*, a "modulator-demodulator" device) would be transmitted using modulation. Ex. 1003 at ¶¶ 235-239. Similarly, any data transmitted via a cellular network would be transmitted using modulation. Ex. 1003 at ¶¶ 235-239. The broadest reasonable interpretation of "modulation" thus would encompass the process of encoding data for transmission over a physical or electromagnetic medium by varying a carrier signal.

IV. Precise Reasons for Relief Requested

A. Claims 1-11, 14-25, and 28-30 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. 1009 at 1. Petitioner submits that claims 1-4, 8-11, 14-16, 21-25, and 28-30 of the '697 patent are unpatentable in view of Ex. 1009 (Beser), considered alone or in conjunction Ex. 1010 (RFC 2401) and knowledge in the field of the '697 patent, for the reasons set forth below, as supported by ¶¶ 255-454 of Ex. 1003.

1. Beser Anticipates Claims 1 and 16

Claims 1 and 16 are defined using the same operative limitations. Claim 1 is cast in the form of a method of connecting devices, while claim 16 is cast in the form of a server system configured to execute the steps of the method defined in claim 1. In this analysis, the steps of the method of claim 1 are first addressed, and then the corresponding system elements of claim 16 are addressed.

Beser (Ex. 1009) 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. 1003 at ¶¶ 255-264, 265-269, 292-293. Beser explains the trusted-third-party network device can be a domain name server. Ex. 1003 at ¶¶ 262-264, 287-291, 306. Beser explains that the first and second network devices may be edge routers, "gateway" computers, cable modems, or other network devices. Ex. 1003 at ¶¶ 261, 280-286. Beser shows the trusted-third-party network device can be a domain name server, and can be one device or a distributed server system. Ex. 1003 at ¶ 290.

To establish an IP tunnel, the originating end device sends a request containing a unique identifier specifying a destination (*i.e.*, a terminating end device). Ex. 1003 at ¶¶ 295-300. The unique identifier can be a domain name. Ex. 1003 at ¶¶ 263, 300, 301. The first network device receives the request, evaluates it, and then sends it to the trusted-third-party network device, if appropriate. Ex. 1003 at ¶¶ 295-296, 309-313. The trusted-third-party network device evaluates the request, and if it corresponds to a terminating device, facilitates a negotiation between the first and second network devices. Ex. 1003 at ¶¶ 302-310. The negotiation involves an exchange of private IP addresses for the originating and terminating end devices that will be used to transmit data between these end devices across a public network. Ex. 1003 at ¶¶ 309-313. The use of these private IP addresses to transmit data over the public network creates a secure,

anonymous tunnel that allows the end devices to directly communicate with each other. Ex. 1003 at ¶¶ 255-259, 265-269, 292-293.

Beser thus shows "*a method of connecting a first network device and a second network device*" as specified in **claim 1**. Ex. 1003 at ¶¶ 345-353. Beser also shows "*A system for connecting a first network device and a second network device, the system including one or more servers*" as specified in **claim 16**. Ex. 1003 at ¶¶ 345-353.

Beser shows that an originating end device will send a request to initiate a tunneling association with a terminating end device, that this request will contain a unique identifier associated with the terminating end device, and that the unique identifier can be a domain name. Ex. 1003 at ¶¶ 299-302. Beser explains that 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. 1003 at ¶¶ 280-286, 295-296. Beser also explains that if the first network device determines a request to initiate an IP tunnel with another end device has been made, it will send the request to the trusted-third-party network device for special processing. Ex. 1003 at ¶¶ 280-286, 295-296, 299-302. After the trusted-third-party network device receives the request containing the domain name (the unique identifier), it looks up the IP address associated with the domain name. Ex. 1003 at ¶¶ 302-308.

Beser thus shows that even though the request contains a unique identifier associated with the terminating end device, the request is actually received initially by the first network device and then by the trusted-third-party network device. Ex. 1003 at ¶¶ 280-286, 295-296, 299-302, 355, 357. Beser also explains that, when the unique identifier is a domain name, the trusted-third-party network device can return to the first network device an IP address associated with a domain name. Ex. 1003 at ¶¶ 305-306. Also, after private network addresses are negotiated, the first network device will inform the originating device of the private IP address associated with the terminating end device. Ex. 1003 at ¶¶ 309-310. Beser thus shows "*intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device*" as specified in **claim 1**. Ex. 1003 at ¶¶ 354-362. Beser thus also shows a server configured to "*intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device*" as specified in **claim 16**. Ex. 1003 at ¶¶ 354-362.

Beser explains that after first network device receives a request, it evaluates it, and if the device determines the packet contains a request to initiate an IP tunnel, it will send the request to the trusted-third-party network device. Ex. 1003 at ¶¶ 280-286, 295-296, 299-302. Beser explains that the trusted-third-party

network device receives the request containing the unique identifier, evaluates it, and takes additional actions based on the results of that evaluation. Ex. 1003 at ¶¶ 260, 262-264, 286-290, 302-308. For example, if the trusted-third-party network device determines the unique identifier specifies a destination that can establish a secure tunnel (*e.g.*, the terminating end device or destination of a VOIP request), it will negotiate with the first and second network devices to establish the IP tunnel between those network devices. Ex. 1003 at ¶¶ 259-260, 302-309. If the domain name sent to the trusted-third-party network device specifies a destination that is unavailable or unknown to the trusted-third-party network device, under the inherent operation of the Beser system, the request will not be routed further. Ex. 1003 at ¶¶ 282-289, 306-308; *see also id.* at ¶¶ 95-118. Beser is able to perform these functions because the trusted-third-party network device stores domain names and associated IP addresses, and may also contain a database of users or end devices. Ex. 1003 at ¶¶ 262-264, 286-290, 302-308.

Beser explains the trusted-third-party network device can be a domain name server located on a public network, and that its systems function according to industry standards. Ex. 1003 at ¶¶ 260, 264, 287-289, 306, 326, 330. Consequently, in the Beser system, 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 inherent function of a DNS server on a public network. Ex. 1003 at ¶¶ 287-289, 305-306; *see also id.* at ¶¶ 95-118. If the trusted-third-party network device returns a public IP address rather than negotiating private IP addresses, the first network device will process traffic from the originating device without attempting to establish a secure IP tunnel. Ex. 1003 at ¶¶ 282-289, 306-308. Consequently, when methods shown in Beser are performed, they will necessarily determine if a second network device is available for secure communications.

Beser thus shows a method comprising the step of "*determining, in response to the request, whether the second network device is available for a secure communications service*" as specified in **claim 1**. Ex. 1003 at ¶¶ 363-370. Beser also therefore shows a server configured to "*determine, in response to the request, whether the second network device is available for a secure communications service*" as specified by **claim 16**. Ex. 1003 at ¶¶ 363-371.

Beser describes processes where, in response to a request containing a unique identifier specifying the location of an end device, the trusted-third-party network device will negotiate with first and second network devices to establish an IP tunnel between the devices. Ex. 1003 at ¶¶ 302-312. This process occurs without any interactions or further action from the user that originally made the request, and is therefore "automatic." Ex. 1003 at ¶¶ 258-260, 307-309.

Beser also explains that after first network device receives a request, it evaluates it, and if the device determines the packet contains a request to initiate an IP tunnel, it will send the request to the trusted-third-party network device. Ex. 1003 at ¶¶ 280-286, 295-296. Beser next shows that the request is received by the trusted-third-party network device, which evaluates the request, compares the identifier to a database of entries, and takes additional actions to establish the IP tunnel based on the results of that evaluation. Ex. 1003 at ¶¶ 302-309. 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. 1003 at ¶¶ 268-270, 303, 303, 318-325. The IP tunnels described in Beser permit end devices to directly communicate over a secure and anonymous channel. Ex. 1003 at ¶¶ 256-259, 266-270, 312-314. Beser thus shows a method comprising the step of "*initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service*" as specified in **claim 1**. Ex. 1003 at ¶¶ 372-376. Beser also therefore shows a system configured to "*initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is*

available for the secure communications service" as specified in **claim 16**. Ex. 1003 at ¶¶ 372-377.

Beser explains that a variety of types of data can be transmitted through an 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. 1003 at ¶¶ 272, 278, 279. These various types of data are audio or audio-video data. Beser thus shows a method "*wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device*" as specified in **claim 1.** Ex. 1003 at ¶¶ 378-381. Beser also therefore shows that the server system is configured such that "*wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device*" as specified in **claim 16**. Ex. 1003 at ¶¶ 378-382.

2. Beser Anticipates Claim 2 and 24

Beser explains that data transmitted through an IP tunnel can represent 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. 1003 at ¶¶ 272, 278, 279. Beser also explains that IP traffic

within an IP tunnel ordinarily will be encrypted using the techniques described in RFC 2401 (*i.e.*, the IPsec protocol). Encryption of traffic sent over an IP tunnel established using IPsec occurs automatically. Ex. 1003 at ¶¶ 268-270, 303, 318-325. Therefore, any VOIP, multimedia, video conference, or other data transmitted through a Beser IP tunnel will be encrypted. Beser thus shows "*The method of claim 1, wherein at least one of the video data and the audio data is encrypted over the secure communication link*" as specified in **claim 2**. Ex. 1003 at ¶¶ 389-391. Beser therefore also shows "*The system of claim 16, wherein at least one of the video data and the audio data is encrypted over the secure communication link*" as specified in **claim 24**. Ex. 1003 at ¶¶ 389-392.

3. Beser Anticipates Claim 3 and 17

Beser anticipates claims 1 and 16, from which claims 3 and 17 depend, respectively. *See* § 1, *above*. Beser shows that the trusted-third-party device, along with the first and second network devices, are used to establish secure IP tunnels. Ex. 1003 at ¶¶ 255-256, 266, 265-269, 292-293. The trusted-third-party network device is connected to a public communication network. Ex. 1003 at ¶¶ 257, 260, 264. Beser shows that its IP tunnels allow end devices to directly communicate over a secure and anonymous channel. Ex. 1003 at ¶¶ 256-259, 266-270, 312-314. Beser explains that IP traffic sent over the public network in an IP tunnel ordinarily is encrypted (*e.g.*, using the IPsec protocol in RFC 2401). Ex.

1003 at ¶¶ 268-270, 303, 318-325. Communications sent between the network devices in the Beser schemes thus ordinarily will be encrypted. *Id.* The broadest reasonable construction of the term "virtual private network communication link" also does not require the traffic sent over the link to be encrypted. *See* § III.C.2, *above*. Beser thus shows "*The method of claim 1, wherein the secure communication link is a virtual private network communication link*" as specified in **claim 3**. Ex. 1003 at ¶¶ 395-400. Beser also shows "*The system of claim 16, wherein the secure communication link is a virtual private network communication link*" as specified in **claim 17**. Ex. 1003 at ¶¶ 395-401.

4. Beser Anticipates Claim 4 and 18

Beser anticipates claims 1 and 16, from which claims 4 and 18 depend, respectively. *See* § 1, *above*. Beser explains that data transmitted through an IP tunnel can represent 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. 1003 at ¶¶ 272, 278, 279. Beser thus shows "*The method of claim 1, wherein the secure communications service includes a video conferencing service*" as specified by **claim 4**. Ex. 1003 at ¶¶ 403-405. Beser also thus shows "*The system of claim 16, wherein the secure communications service includes a video conferencing service*" as specified in **claim 18**. Ex. 1003 at ¶¶ 403-406.

5. Beser Anticipates Claims 5, 6, 7, 19, 20, and 21

Beser anticipates claims 1 and 16, from which claims 5 and 19 depend, respectively. *See* § 1, *above*. Beser explains that data transmitted through an IP tunnel can represent VOIP traffic or video conference traffic. Ex. 1003 at ¶¶ 272, 278, 279. Beser thus shows "*The method of claim 1, wherein the secure communications service includes a telephony service*" as specified by **claim 5**. Ex. 1003 at ¶¶ 407-409. Beser also therefore shows "*The system of claim 16, wherein the secure communications service includes a telephony service*" as specified by **claim 19**. Ex. 1003 at ¶¶ 407-410.

Claims 6 and 20 specify the method of claim 5 or the system of claim 16, respectively, "*wherein the telephony service uses modulation*." Claims 7 and 21 recite the method of claim 6 or the system of claim 20, and 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, Ex. 1003 at ¶¶ 272, 278, 279, and shows several examples of devices that can be used to transmit such data. For example, Beser explains that the first and second network device each can be a cable modem. 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. 1003 at ¶¶ 170-176. 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. 1003 at ¶¶ 272-277. Data transmitted to a mobile device using WAP necessarily would have been transmitted over a wireless network, such as a GSM network (which employed TDM) or a CDMA network. Ex. 1003 at ¶ 276.

Beser thus shows a method or system "*wherein the telephony service uses modulation*" as specified by **claim 6** and **claim 20**, respectively. Ex. 1003 at ¶¶ 411-414. Beser also shows a method or system "*wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA)*" as specified by **claim 7** and **claim 21**, respectively. Ex. 1003 at ¶¶ 416-419. Additionally, Petitioner notes that **claim 20** (and therefore **claim 21**) is indefinite, as there is no antecedent basis for term "*the telephony service*" in these claims.

6. Beser Anticipates Claim 8, 9, 22 and 23

Beser anticipates claims 1 and 16, from which claims 8 and 22 depend, respectively. *See* § 1, *above*. Beser 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 WAP Forum.

Ex. 1003 at ¶¶ 272-277. Data transmitted to a mobile device using WAP necessarily would have been transmitted over a wireless network. Ex. 1003 at ¶ 276. Beser thus shows "*The method of claim 1, wherein at least one of the first network device and the second network device is a mobile device*" as specified in **claim 8**. Ex. 1003 at ¶¶ 421-422. Beser thus also shows "*The system of claim 16, wherein at least one of the first network device and the second network device is a mobile device*" as specified in **claim 22**. Ex. 1003 at ¶¶ 421-423.

Claims 9 and 23 specify that the mobile device in claims 8 and 22 is a "*notebook computer*." A laptop or notebook computer is a type of personal computer. Ex. 1003 at ¶ 272. Beser thus shows "*The method of claim 8, wherein the mobile device is a notebook computer*" as specified in **claim 9**. Ex. 1003 at ¶¶ 424-426. Beser also shows "*The system of claim 22, wherein the mobile device is a notebook computer*" as specified in **claim 23**. Ex. 1003 at ¶¶ 424-427.

7. Beser Anticipates Claim 10 and 29

Beser anticipates claims 1 and 16, from which claims 10 and 29 depend, respectively. *See* § 1 *above*. Beser further explains that an originating device will send a request to initiate a tunneling association with a terminating end device, that the request will contain a unique identifier associated with the terminating end device, and that the unique identifier can be a domain name. Ex. 1003 at ¶¶ 299-302. Beser explains that the request is initially received by a first network device,

which evaluates the request and sends it to the trusted-third-party network device if appropriate. Ex. 1003 at ¶¶ 280-286, 299-302. The first network device and the trusted-third-party network device are distinct devices relative to the intended target of the request (*i.e.*, the terminating end device). Ex. 1003 at ¶ 260. The trusted-third-party network device can be a domain name server, and its functionality can be distributed over multiple devices on the network. Ex. 1003 at ¶¶ 262-265, 287-291, 302-308. Beser explains that after the trusted-third-party network device receives the request, it looks up an IP address associated with the unique identifier. Ex. 1003 at ¶¶ 302-308.

Under the inherent operation of the Beser process, if a domain name specifies a destination that is unavailable or unknown to the trusted-third-party network device, the request will not be routed further. Ex. 1003 at ¶¶ 282-289, 306-308; *see also id.* at ¶¶ 95-118. Beser thus shows "*The method of claim 1, wherein intercepting the request consists of receiving the request to determine whether the second network device is available for the secure communications service*" as specified by **claim 10**. Ex. 1003 at ¶¶429-434. Beser thus also shows "*The system of claim 16, wherein the one or more servers are configured to intercept the request by receiving the request to determine whether the second network device is available for the secure communications service*" as specified in **claim 29**. Ex. 1003 at ¶¶ 429-435.

8. Beser Anticipates Claim 11 and 25

Beser anticipates claims 1 and 16, from which claims 11 and 25 depend, respectively. *See* § 1 *above*. Beser describes methods and systems that create IP tunnels between two network devices using a trusted-third-party network device. IP tunnels are secure tunnels established over the Internet. Ex. 1003 at ¶¶ 255-258. Transmission of data via TCP/IP necessarily involves transmission of data packets over a network. Ex. 1003 at ¶¶ 67-74. Beser thus shows "*The method of claim 1, wherein the secure communication link supports data packets*" as specified in **claim 11**. Ex. 1003 at ¶¶ 436-438. Beser thus also shows "*The system of claim 16, wherein the secure communication link supports data packets*" as specified in **claim 25**. Ex. 1003 at ¶¶ 436-439.

9. Beser Anticipates Claim 14 and 28

Beser anticipates claims 1 and 16, from which claims 14 and 28 depend, respectively. *See* § 1, *above*. As explained therein, Beser describes processes where, in response to a request containing a unique identifier specifying the location of an end device, a trusted-third-party network device will evaluate the request, compare the identifier to a database of entries, and take additional actions to establish the IP tunnel based on the results of that evaluation. Ex. 1003 at ¶¶ 260, 262-264, 286-290, 302-308. Beser further explains that the unique identifier in a request is associated with the terminating device, and can be a

domain name. Ex. 1003 at ¶¶ 299-302. Beser explains that the trusted-third party network device can be a domain name server that stores the domain names and associated IP addresses, and may be configured to contain a database of users or end devices. Ex. 1003 at ¶¶ 262-264, 286-290, 302-308.

Beser shows that the trusted-third-party network device will determine if a unique identifier corresponds to a terminating end device, and if so, will negotiate with first and second network devices to establish an IP tunnel between the first and second network devices. Ex. 1003 at ¶¶ 302-312. The trusted-third-party network device evaluates the domain name in a request, and, if appropriate, will resolve the domain name in the request. Ex. 1003 at ¶¶ 302-309. These steps, individually or together, determine if a destination specified in a request is available for secure communications. For example, if a domain name sent to the trusted-third-party network device specifies a destination that is unavailable or unknown to the trusted-third-party network device, the request will not be routed further and an error message will be returned. Ex. 1003 at ¶¶ 282-289, 306-308; *see also id.* at ¶¶ 95-118. Similarly, if the domain name 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, by its nature of being a domain name server, simply return the IP address associated with the (non-secure) domain. Ex. 1003 at ¶¶ 287-289, 305-306; *see also id.* at ¶¶ 95-

118. Conversely, if the domain name is recognized by the trusted-third-party network device, and maps to a terminating end device, an IP tunnel will be established. Beser thus shows "*The method of claim 1, wherein determining that the second network device is available for a secure communications service is a function of a domain name lookup*" as specified in **claim 14**. Ex. 1003 at ¶¶ 440-448. Beser thus also shows "*The system of claim 16, wherein the determination that the second network device is available for the secure communications service is a function of the result of a domain name lookup*" as specified in **claim 28**. Ex. 1003 at ¶¶ 440-449.

10. Beser Anticipates Claim 15 and 30

Beser anticipates claims 1 and 16, from which claims 15 and 30 depend, respectively. *See* § 1 *above*. As Beser explains that an originating device will send a request to initiate a tunneling association with a terminating device. The request will contain a unique identifier associated with the terminating device, and that the unique identifier can be a domain name. Ex. 1003 at ¶¶ 299-302. The request is initially received by a first network device, which may then send the request to the trusted-third-party network device. Ex. 1003 at ¶¶ 280-286. Beser shows that the request containing the unique identifier is received by the trusted-third-party network device, which is a separate device from the originating device. Ex. 1003 at ¶¶ 299-302, 260-262. Beser also shows that the first network device may be

separate from the originating device. Ex. 1003 at ¶¶ 260-262. Beser thus shows "*The method of claim 1, wherein intercepting the request occurs within another network device that is separate from the first network device*" as specified in **claim 15**. Ex. 1003 at ¶¶ 450-453. Beser thus also shows "*The system of claim 16, wherein the one or more servers configured to intercept the request are separate from the first network device*" as specified in **claim 30**. Ex. 1003 at ¶¶ 450-454.

B. Beser In View of RFC 2401 Renders Obvious Claims 1-11, 14-25, and 28-30

Claims 1-11, 14-25, and 28-30 are anticipated by Beser for the reasons set forth in §§ IV.A.1 to IV.A.10, 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 and 16 to have been obvious in February of 2000 based on Beser in view of RFC 2401.

1. Claims 2 and 24 Would Have Been Obvious

Claims 2 and 24 depend from claims 1 and 16, respectively, and each specify that "*at least one of the video data and the audio data **is encrypted** over the secure communication link*." In proceedings involving other patents in the same family as the '697 patent, Patent Owner has asserted that a VPN requires data sent via the VPN to be encrypted, and that Beser does not show encryption of traffic sent via IP tunnels. *See, e.g.*, Ex. 1056 at 24-26.

Should Patent Owner contend that a "secure communication link" requires all data sent via the link to be encrypted and that Beser does not show this element, those contentions should be rejected for several reasons.

First, as explained in § III.C.2, above, a "secure communication link" cannot be construed in its broadest reasonable construction to require traffic to be encrypted. This is because dependent claims 2 and 24 expressly specify that the data sent over the secure communication link must be encrypted, which, under the doctrine of claim differentiation, means that claims 1 and 16 in their broadest reasonable construction do not require this condition to be true.

Second, Beser clearly teaches that IP tunnels ordinarily encrypt traffic sent through the tunnel, and uses encryption to establish such tunnels even in the particular applications where Beser suggests that encryption may not be used due to practical requirements of a particular computer implementation. Ex. 1003 at ¶¶ 268-270, 303, 318-325.

Third, as explained in § IV.A.1, Beser does show use of encryption in its IP tunneling solutions, even in high data volume applications. 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. 1003 at ¶ 325. Beser also explains that encryption is ordinarily to be used in IP tunnels other than in two specific situations involving high volume data

transfers and equipment that cannot handle the encryption of that volume of traffic. Ex. 1003 at ¶¶ 268-270, 303, 318-325.

If the Board does not find claims 2 and 24 anticipated by Beser, a person of ordinary skill in the art would have considered encrypting traffic in the Beser IP tunneling systems to have been obvious based on RFC 2401 (Ex. 1010). Initially, a person of ordinary skill would have considered Beser in conjunction with RFC 2401 because Beser expressly refers to the IPsec protocol (which is defined in RFC 2401) as being the conventional way that IP tunnels it is describing are established. Ex. 1003 at ¶¶ 269-270, 330. A person of ordinary skill, based on the guidance in Beser, would have been motivated to incorporate encryption in IP tunneling schemes, as this is the practice that Beser identifies is typically followed. Ex. 1003 at ¶¶ 268-270, 318-325. Indeed, Beser states encryption ordinarily is to be used in IP tunnels, and identifies a particular technique (IPsec) that encrypts network traffic sent via IP tunnels. Ex. 1003 at ¶¶ 268-270, 318-325. 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. 1003 at ¶¶ 260, 264, 287-291, 320, 326-331.

RFC 2401 explains, under the IPsec protocol, network traffic is automatically encrypted as it is sent through security gateways over a public network. Ex. 1003 at ¶¶ 333-343. RFC 2401 also explains in the IPsec scheme, IP

traffic is evaluated and necessary encryption is added to the appropriate packets. Ex. 1003 at ¶¶ 336-339. 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. 1003 at ¶¶ 145, 336-340.

A person of ordinary skill also would have recognized IPsec could be readily integrated into the Beser systems. Ex. 1003 at ¶¶ 269, 341-342, 384-386. 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. 1003 at ¶¶ 260-261, 280-286, 337-343.

Notably, none of the claims of the ’697 patent are limited to the “high volume”/“low equipment capacity” scenario that was the subject of the Beser concerns. 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 ’697 claims are not limited to situations where that hypothetical concern would be relevant. More directly, a person of ordinary skill would have immediately recognized there was a common sense solution to the capacity problem identified in Beser; namely, use of more powerful edge routers or gateway computers or reducing the quality of the digitized voice call or multimedia data to decrease the amount of data that must be encrypted. Ex. 1003 at ¶ 388.

In addition, a person of ordinary skill would have found a direct suggestion to encrypt all network traffic being sent through Beser IP tunnels from the combined teachings of Beser and RFC 2401. Ex. 1003 at ¶¶ 326-331, 341-343. RFC 2401 explains that under the IPsec standard, all traffic sent over secure IP tunnels is automatically encrypted. Ex. 1003 at ¶ 337. 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. 1003 at ¶¶ 334-337. RFC 2401 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. 1003 at ¶¶ 342-343. Thus, a person of ordinary skill would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling schemes because that is what RFC 2401 says to do with IP tunnels configured in its "case 3" design. Ex. 1003 at ¶ 341. Beser considered in view of RFC 2401, thus, would have rendered claims 2 and 24 obvious to a person of ordinary skill in the art in February of 2000. Ex. 1003 at ¶¶ 384-388.

2. Dependent Claims 3 and 17 Would Have Been Obvious

Beser anticipates claims 3 and 17 for the reasons set forth in § IV.A.3, above. Patent Owner may contend that Beser does not describe the creation of a VPN because it does not disclose encryption of all IP packets sent through its IP

tunnels. This distinction, even if established, would not render claims 3 or 17 patentable.

As explained above, a person of ordinary skill would have found it obvious to encrypt all network traffic being sent through Beser IP tunnels based on the combined teachings of Beser and RFC 2401. *See* § 1, *above*. Because Beser itself describes systems and processes meeting the requirements of each of claims 3 and 17, each of those claims also would have been considered obvious by a person of ordinary skill in February of 2000 based on the combined teachings of Beser and RFC 2401 for the reasons in § IV.A.3, above.

3. Claims 1, 16, 4-11, 16, 18-23, 25, and 28-30 Would Have Been Obvious

Should the Board determine that claims 1 and 16 require network traffic to be encrypted, and that Beser does not anticipate these claims on that basis, then Beser considered in view of RFC 2401 would have rendered claims 1 and 16 obvious for the reasons set forth in § 1, above.

Also, because Beser also describes systems and processes meeting the requirements of each of claims 4-11, 16, 18-23, 25, and 28-30, each of those claims would have been considered obvious by a person of ordinary skill in February of 2000 based on the combined teachings of Beser and RFC 2401 for the reasons in §§ IV.A.1-IV.A.10, above.

C. Claims 1-11, 14-25, and 28-30 Are Anticipated by RFC 2543

RFC 2543 (Ex. 1012) was published before March 1999, and is prior art under at least under §102(a). Petitioner submits that claims 1-4, 8-11, 14-16, 21-25, and 28-30 of the '697 patent are unpatentable in view of Ex. 1012 (RFC 2453), considered alone or in conjunction with Exhibits 1013 (RFC 1889), 1014 (RFC 2327), 1015 (Mobility Support Using SIP) and knowledge in the field of the '697 patent, for the reasons below and at ¶¶ 456-538 of Ex. 1003.

1. RFC 2543 Anticipates Claims 1 and 16

Claims 1 and 16 are defined using the same operative limitations. Claim 1 is cast in the form of a method of connecting devices, while claim 16 is cast in the form of a server system configured to execute the steps of the method defined in claim 1. In this analysis, the steps of the method of claim 1 are first addressed, and then the corresponding system elements of claim 16 are addressed.

RFC 2543 describes the Session Initiation Protocol (SIP), a standard promulgated by the Internet Engineering Task Force ("IETF"). The SIP protocol was developed through extensive deliberations, and reflects well-known and accepted principles for designing call signaling mechanisms applicable to establishing multimedia communications between devices over a network. Ex. 1003 at ¶¶ 456-458. RFC 2543 describes methods and systems for establishing multimedia "sessions" between a caller and one or more callees. Ex. 1003 at

¶¶ 447, 456-463. RFC 2543 shows that a "session" "include[s] Internet multimedia conferences, Internet telephone calls and multimedia distribution." Ex. 1003 at ¶ 457 (quoting Ex. 1012 at 1, 7).

SIP was designed as a suite of protocols for transmitting multimedia data. Ex. 1003 at ¶¶ 456-458, 472. SIP includes protocols governing the exchange of messages for initiating, managing, and terminating a call or a session. Ex. 1003 at ¶¶ 456-457. The SIP architecture includes several devices, including: at least two SIP user agents (*e.g.*, software for a SIP client), one or more SIP servers (*e.g.*, proxy servers or redirection servers), and one or more location servers. Ex. 1003 at ¶¶ 474-475. A party is identified by a SIP address also called a "SIP URL." Ex. 1003 at ¶ 479. SIP URLs take the form of "user@domain name" or "user@IP address". Ex. 1003 at ¶¶ 479-480. For example, "sip:j.doe@big.com" and "sip:alice@example.com" would be SIP URLs. Ex. 1003 at ¶ 479 (quoting Ex. 1012 at 24). The location servers allow a user to switch locations and still receive calls by enabling a user to register its SIP URL and present location with the server. Ex. 1003 at ¶¶ 475, 481-486.

RFC 2543 shows that to initiate a call a caller creates an INVITE message containing a callee's SIP URL. Ex. 1003 at ¶¶ 490-492. The SIP URL may contain a domain name. Ex. 1003 at ¶¶ 490-493. A local SIP proxy server can receive the INVITE message and handle setting up the call for the caller. Ex. 1003

at ¶¶ 494, 495, 502. The proxy server will locate the SIP server associated with the callee's domain by querying a DNS server. Ex. 1003 at ¶¶ 495-502. The proxy server then will send the INVITE message to an IP address returned by the DNS server. Ex. 1003 at ¶¶ 495-502.

RFC 2543 shows that the callee's SIP server will receive the INVITE message and then attempt to locate the callee. Ex. 1003 at ¶ 503. The server locates the callee by querying a location server to determine whether the callee is available. Ex. 1003 at ¶¶ 481-486, 503. If the callee is available, the location server will return the address presently associated with the callee's location (*i.e.*, the address the callee registered with the server). *Id.* The callee's SIP server then will send the INVITE message to the callee. Ex. 1003 at ¶¶ 459-461, 490-499, 502-505. The callee will receive the INVITE message and will send a response back to the caller. Ex. 1003 at ¶¶ 499-506. If the callee accepts the call, the response message will contain a success status indicator code. Ex. 1003 at ¶¶ 506-507. If the caller receives a message indicating the callee accepted the call, the caller will return an ACK message to the callee. Ex. 1003 at ¶¶ 511-512. The caller and callee then can exchange multimedia data. Ex. 1003 at ¶¶ 461, 472-473, 512. The call will continue until it is terminated. Ex. 1003 at ¶ 513. For a two-party call, either caller or callee can terminate the call by transmitting a BYE message. Ex. 1003 at ¶ 514.

RFC 2543 thus shows "*A method of connecting a first network device and a second network device*" as specified in **claim 1**. Ex. 1003 at ¶¶ 545-553. RFC 2543 thus also shows "*A system for connecting a first network device and a second network device, the system including one or more servers*" as specified in **claim 16**. Ex. 1003 at ¶¶ 545-555.

RFC 2543 shows that to start the process for initiating a call, the caller creates an INVITE message. Ex. 1003 at ¶¶ 490-492. The caller addresses the message to a callee by putting the callee's SIP address in the "To" and the "Request-URI" header fields. Ex. 1003 at ¶¶ 492-493. The caller can specify request that the call will include both audio and video data, or just one or other. Ex. 1003 at ¶¶ 461-462. The caller also may specify that SIP messages be encrypted by setting the "Encryption" header field of the INVITE message. Ex. 1003 at ¶¶ 461-465, 468, 531-537. The caller may set other options in the INVITE message, such as setting a proxy server for SIP messages. Ex. 1003 at ¶¶ 531-537.

Even though an INVITE message is addressed to the callee, RFC 2543 shows that the SIP environment may be configured so that the INVITE message will be intercepted by a local SIP proxy server that handles setting up the call for the caller. Ex. 1003 at ¶¶ 492, 495. The local SIP proxy server will locate the SIP server associated with the callee's domain by querying a DNS server. Ex. 1003 at ¶¶ 495, 498-502, 523-524. The proxy server will then send the INVITE message

to the callee's SIP server using the IP address returned by the DNS server. Ex. 1003 at ¶¶ 498-502. The callee's SIP server will attempt to locate the callee by querying a location server. Ex. 1003 at ¶¶ 503, 518, 525. If the callee is available the location server will return the callee's current address. Ex. 1003 at ¶¶ 481-486. The callee's SIP server then may send the INVITE message to the callee, or it may return a redirect message to the caller. Ex. 1003 at ¶¶ 503-505, 510. Thus, RFC 2543 shows the callee's SIP server also intercepts the INVITE message. Ex. 1003 at ¶¶ 503-506, 510, 515-522, 565.

RFC 2543 thus shows "*intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device*" as specified in **claim 1**. Ex. 1003 at ¶¶ 556-567. RFC 2543 also therefore shows a server configured to "*intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device*" as specified in **claim 16**. Ex. 1003 at ¶¶ 556-567.

RFC 2543 explains that after the caller sends the INVITE message, the callee's SIP server will receive the message, and then try to locate the callee. Ex. 1003 at ¶ 503; *see id.* at ¶¶ 481-486, 503-510. The callee's SIP server will locate the callee by querying a location server. Ex. 1003 at ¶¶ 503, 518, 525. If the callee has registered with the location server, the location server may return the IP

address associated with the callee or it may return a hostname. Ex. 1003 at ¶¶ 481-486. If it returns a hostname, the callee's SIP server will resolve the callee's address into an IP address by querying a DNS server. Ex. 1003 at ¶¶ 503, 518, 525.

In some instances, the callee's SIP server may return an error message. If the callee's SIP server cannot locate the callee (*e.g.*, because the callee has not registered with the location server), it will return an error message (*e.g.*, "404 Not Found"). Ex. 1003 at ¶¶507, 509-510. Also, if the SIP server knows the callee cannot generate a response that has characteristics acceptable to the caller, it will return an error message (*e.g.*, "406 Not Acceptable" or "606 Not Acceptable"). Ex. 1003 at ¶¶ 485, 528-530, 536. For example, one of the call parameters is whether the communications are to be encrypted. Ex. 1003 at ¶¶ 460-472. The "Encryption" field of the INVITE message indicates whether the content of message has been encrypted. Ex. 1003 at ¶¶ 460-472. One reason the message would be encrypted is that the SIP message specifies the encryption key or keys to be used to encrypt session data. Ex. 1003 at ¶¶ 460-472. To ensure those keys are not retransmitted back to the caller in the clear, the caller can require that all SIP messages be encrypted. Ex. 1003 at ¶¶ 531-537. If an INVITE message specifies that SIP messages must be encrypted, and the callee cannot support encryption, the callee's SIP server will return an error message. Ex. 1003 at ¶¶ 460-472, 531-537.

If the callee is found, the callee's SIP server will send the INVITE message to the IP address associated with the callee. Ex. 1003 at ¶¶ 479, 486, 503-504, 518. The callee will receive the INVITE message and will send a response back to the caller. Ex. 1003 at ¶¶ 506, 508, 519. If the callee accepts the call, the response message will contain a success status indicator code. Ex. 1003 at ¶¶ 508, 511, 519. The callee may accept all the call parameters proposed by the caller or it may accept only some parameters to be used during the call (*e.g.*, accept the audio stream but reject the video stream). Ex. 1003 at ¶¶ 528-530. If the callee rejects the call, the response message will contain an error status indicator code (*e.g.*, "600 Busy Everywhere" or "606 Not Acceptable"). One reason it may reject the call is if the caller has specified call parameters that the callee cannot support. Ex. 1003 at ¶¶ 509, 510, 530, 536. For example, if the INVITE message requires encryption and the callee is unable to support the requested encryption, an error message is returned. Ex. 1003 at ¶ 536.

RFC 2543 thus shows a method comprising the step of "*determining, in response to the request, whether the second network device is available for a secure communications service*" as specified in **claim 1**. Ex. 1003 at ¶¶ 568-583. RFC 2543 also therefore shows a server configured to "*determine, in response to the request, whether the second network device is available for a secure communications service*" as specified in **claim 16**. Ex. 1003 at ¶¶ 568-583.

RFC 2543 explains that to start the process for initiating a call, the caller will create and transmit to the callee an INVITE message. Ex. 1003 at ¶¶ 490-492. The caller will specify the call parameters by including a SDP session description in the message body of the INVITE message. Ex. 1003 at ¶¶ 460-472, 491, 527, 531, 537. One of the parameters that can be specified in the session description is the encryption key to be used to encrypt session data. Ex. 1003 at ¶¶ 461-465, 531-537. If the session description contains an encryption key, the INVITE message will be encrypted with a public key associated with callee. Ex. 1003 at ¶¶ 527-537. The caller will specify that the message is encrypted by setting the "Encryption" field of the INVITE message, and the caller also should specify in the Response-Key field another key to use to encrypt future SIP messages. Ex. 1003 at ¶¶ 531-537.

If the callee accepts the call, the response message will contain a success status indicator code. Ex. 1003 at ¶¶ 508, 511, 519. The callee will encrypt the response with the key identified in the Response-Key field of the INVITE message. Ex. 1003 at ¶¶ 531-537. If the callee accepted the call, the caller will return an ACK message to the callee. Ex. 1003 at ¶¶ 511-512. Based on the call parameters specified during this process, the caller and callee then begin to exchange multimedia data. Ex. 1003 at ¶¶ 512-514. If the caller and callee agreed to using a session encryption key, the session data streams will be encrypted

according to the parameters established during the call initiation process. Ex. 1003 at ¶¶ 460-472, 512-514.

RFC 2543 thus shows a method comprising the step of "*initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service*" as specified in **claim 1**. Ex. 1003 at ¶¶ 584-592. RFC 2543 thus also shows a system configured to "*initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service*" as specified in **claim 16**. Ex. 1003 at ¶¶ 584-592.

RFC 2543 explains that SIP is a control protocol for creating, modifying and terminating "sessions," which "include Internet multimedia conferences, Internet telephone calls and multimedia distribution." Ex. 1003 at ¶¶ 459-460, 462-463. RFC 2543 thus shows a method "*wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device*" as specified in **claim 1**. Ex. 1003 at ¶¶ 593-595. RFC 2543 also therefore shows that the server system is configured such that "*wherein the secure communications service uses the secure communication link to communicate at least one of video*

data and audio data between the first network device and the second network device" as specified in **claim 16**. Ex. 1003 at ¶¶ 593-595.

2. RFC 2543 Anticipates Claim 2 and 24

RFC 2543 anticipates claims 1 and 16, from which claims 2 and 24 depend, respectively. *See* § 1, *above*. RFC 2543 shows that SIP is a control protocol for creating, modifying and terminating "sessions," which "include Internet **multimedia conferences**, Internet **telephone calls** and **multimedia distribution**." Ex. 1003 at ¶ 457 (quoting Ex. 1012 (RFC 2543) at 1, 7) (emphasis added); *see* Ex. 1003 at ¶¶ 459-460, 462-463. In a SIP call, each data stream is transmitted in a separate session. Ex. 1003 at ¶ 463 ("In a multimedia session, each medium is carried in a separate RTP session . . ." (quoting Ex. 1013 at 8)).

RFC 2543 explains session data sent in a call can be encrypted. Ex. 1003 at ¶¶ 460-472, 491, 527, 531, 537. The caller can vary the granularity of the encryption being used in a call. For example, a caller can specify one key to use for all content (*e.g.*, one key for both audio and video streams) within the call, or different keys for each session (*e.g.*, a different key for each audio and video stream) within the call. Ex. 1003 at ¶¶ 464-465, 532, 537, 605. The caller also may specify a key for some but not all sessions. *Id.* Based on the call parameters specified during the call setup process, the caller and callee then begin to exchange multimedia data. Ex. 1003 at ¶ 512. If the session description specified an

encryption key to be used for a particular session, that session will be encrypted. Ex. 1003 at ¶¶ 463-469, 531. RFC 2543 thus shows "*The method of claim 1, wherein at least one of the video data and the audio data is encrypted over the secure communication link*" as specified by **claim 2**. Ex. 1003 at ¶¶ 601-609. RFC 2543 therefore also shows "*The system of claim 16, wherein at least one of the video data and the audio data is encrypted over the secure communication link*" as specified by **claim 24**. Ex. 1003 at ¶¶ 601-609.

3. RFC 2543 Anticipates Claim 3 and 17

RFC 2543 anticipates claims 1 and 16, from which claims 3 and 17 depend, respectively. *See* § 1, *above*. RFC 2543 shows that the caller and the callee are connected to a public communication network such as the Internet. Ex. 1003 at ¶¶ 457, 460, 477-478, 496. A caller can specify in the session description the encryption key or keys to be used to encrypt session data. Ex. 1003 at ¶¶ 463-469, 531. RFC 2543 also shows that the SIP proxy servers can be configured to encrypt parts of the SIP messages to hide the identities of the caller and callee. Ex. 1003 at ¶¶ 540-542, 611. RFC 2543 shows that after a call has been initiated the caller and all callees may directly communicate over a secure and anonymous channel. Ex. 1003 at ¶¶ 512-514, 532-543. A secure and anonymous channel is a VPN under the broadest reasonable construction of the claims. *See* § III.C.2.

RFC 2543 thus shows "*The method of claim 1, wherein the secure communication link is a virtual private network communication link*" as specified by **claim 3**. Ex. 1003 at ¶¶ 610-615. RFC 2543 thus shows "*The system of claim 16, wherein the secure communication link is a virtual private network communication link*" as specified by **claim 17**. Ex. 1003 at ¶¶ 610-615.

4. RFC 2543 Anticipates Claim 4 and 18

RFC 2543 anticipates claims 1 and 16, from which claims 4 and 18 depend, respectively. *See* § 1, *above*. RFC 2543 explains that SIP is a control protocol for creating, modifying and terminating "sessions," which "include Internet multimedia conferences, Internet telephone calls and multimedia distribution." Ex. 1003 at ¶ 457. A multimedia conference may be a video conference. Ex. 1003 at ¶ 616. RFC 2543 thus shows "*The method of claim 1, wherein the secure communications service includes a video conferencing service*" as specified by **claim 4**. Ex. 1003 at ¶¶ 616-618. RFC 2543 thus also shows "*The system of claim 16, wherein the secure communications service includes a video conferencing service*" as specified by **claim 18**. Ex. 1003 at ¶¶ 616-618.

5. RFC 2543 Anticipates Claim 5, 6, 7, 19, 20, and 21

RFC 2543 anticipates claims 1 and 16, from which claims 5 and 19 depend, respectively. *See* § 1, *above*. RFC 2543 explains that SIP is a control protocol for creating, modifying and terminating "sessions," which "include Internet

multimedia conferences, Internet telephone calls and multimedia distribution." Ex. 1003 at ¶ 457. RFC 2543 thus shows "*The method of claim 1, wherein the secure communications service includes a telephony service*" as specified by **claim 5**. Ex. 1003 at ¶¶ 619-621. RFC 2543 thus also shows "*The system of claim 16, wherein the secure communications service includes a telephony service*" as specified by **claim 19**. Ex. 1003 at ¶¶ 619-621.

Claims 6 and 20 specify, respectively, that the method of claim 5 or the system of claim 16 further comprises: "*wherein the telephony service uses modulation*." Claims 7 and 21 specify, respectively, the method of claim 6 or the system of claim 20 further comprises that "*the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA)*".

RFC 2543 shows that SIP may be used to make Internet to Public Switched Telephone Network (PSTN) calls. Ex. 1003 at ¶ 478. Voice data transmitted over a PSTN inherently is modulated using TDM. Ex. 1003 at ¶ 189. RFC 2543 also shows that the caller or the callee may use a mobile device such as a mobile phone or PDA. Ex. 1003 at ¶ 487. Data transmitted to a mobile device necessarily would have been transmitted over a wireless network, such as a GSM network (which employed TDM) or a CDMA network. Ex. 1003 at ¶¶ 272-277. Both network types use modulation. RFC 2543 thus shows a method or system "*wherein the*

telephony service uses modulation" as specified by **claims 6 and 20**. Ex. 1003 at ¶¶ 622-624. RFC 2543 also shows a method or system "*wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA)*" as specified by **claims 7 and 21**. Ex. 1003 at ¶¶ 625-627.

6. RFC 2543 Anticipates Claim 8, 9, 22, and 23

RFC 2543 anticipates claims 1 and 16, from which claims 8 and 22 depend, respectively. *See* § 1, *above*. RFC 2543 shows that the caller or the callee may use a mobile device such as a PDA, laptop, or mobile phone. Ex. 1003 at ¶ 487. RFC 2543 thus shows "*The method of claim 1, wherein at least one of the first network device and the second network device is a mobile device*" as specified by **claim 8**. Ex. 1003 at ¶¶ 628-630. RFC 2543 thus also shows "*The method of claim 8, wherein the mobile device is a notebook computer*" as specified by **claim 9**. Ex. 1003 at ¶¶ 632-634. RFC 2543 also shows "*The system of claim 16, wherein at least one of the first network device and the second network device is a mobile device*" as specified by **claim 22**. Ex. 1003 at ¶¶ 628-630. RFC 2543 thus also shows "*The system of claim 22, wherein the mobile device is a notebook computer*" as specified by **claim 23**. Ex. 1003 at ¶¶ 632-634.

7. RFC 2543 Anticipates Claim 10 and 29

RFC 2543 anticipates claims 1 and 16, from which claims 10 and 29 depend, respectively. *See* § 1, *above*. RFC 2543 shows that a caller's proxy server will receive an INVITE message addressed to a callee. Ex. 1003 at ¶¶ 495, 502, 503. The proxy server will determine whether the callee is available by querying another SIP proxy server. Ex. 1003 at ¶¶ 499-502. RFC 2543 also shows that the callee's proxy server then will receive the INVITE message addressed to a callee. Ex. 1003 at ¶¶ 495, 502, 503. The calee's proxy server will determine whether the callee is available by querying a location server. Ex. 1003 at ¶ 503. Because the INVITE messages are received by the proxy servers rather than the callee/caller, they are intercepted within the meaning of the claims. *See* § III.C.4. RFC 2543 thus shows "*The method of claim 1, wherein intercepting the request consists of receiving the request to determine whether the second network device is available for the secure communications service*" as specified by **claim 10**. Ex. 1003 at ¶¶ 636-639. RFC 2543 thus also shows "*The system of claim 16, wherein the one or more servers are configured to intercept the request by receiving the request to determine whether the second network device is available for the secure communications service*" as specified by **claim 29**. Ex. 1003 at ¶¶ 636-639.

8. RFC 2543 Anticipates Claim 11 and 25

RFC 2543 anticipates claims 1 and 16, from which claims 11 and 25 depend, respectively. *See* § 1, *above*. RFC 2543 shows that data can be transmitted via the TCP or UDP connection established between the caller and the callee. Ex. 1003 at ¶¶ 496, 640. TCP and UDP send data via IP packets. Ex. 1003 at ¶¶ 68-69. RFC 2543 thus shows "*The method of claim 1, wherein the secure communication link supports data packets*" as specified by **claim 11**. Ex. 1003 at ¶¶ 640-642. RFC 2543 thus also shows "*The system of claim 16, wherein the secure communication link supports data packets*" as specified by **claim 25**. Ex. 1003 at ¶¶ 640-642.

9. RFC 2543 Anticipates Claim 14 and 28

RFC 2543 anticipates claims 1 and 16, from which claims 14 and 28 depend, respectively. *See* § 1, *above*. RFC 2543 explains that to start the process for initiating a call, the caller creates an INVITE message that contains the callee's SIP URL. Ex. 1003 at ¶¶ 490-492. The SIP URL may contain a domain name. Ex. 1003 at ¶¶ 490-493. The INVITE message may be received by a local SIP proxy server that will handle setting up the call for the caller. Ex. 1003 at ¶¶ 494, 495, 502.

RFC 2543 shows that the local SIP proxy server will determine whether a callee is available by querying a SIP proxy server that is associated with callee's domain. Ex. 1003 at ¶¶ 499-502. The local SIP proxy server will locate a SIP

server associated with the callee's domain by querying a DNS server. Ex. 1003 at ¶¶ 495, 498-502, 523-524. The proxy server then will send the INVITE message to an IP address returned by the DNS server. Ex. 1003 at ¶¶ 504, 516-519, 523-526.

The callee's proxy server will determine whether the callee is available by querying a location server. Ex. 1003 at ¶ 503. If the callee is available, the location server will return the address presently associated with the callee's location. Ex. 1003 at ¶¶ 481-486, 503. If the address contains an IP address, the proxy server will send the message to the callee. Ex. 1003 at ¶¶ 481-486, 503-504, 516-519, 523-526. If it contains a domain name, the proxy server will query a DNS server, and then use the IP address to send the message to the callee. Ex. 1003 at ¶¶ 504, 516-519, 523-526. If either proxy server cannot locate the callee, it will return an error message. Ex. 1003 at ¶¶ 507, 510.

RFC 2543 thus shows "*The method of claim 1, wherein determining that the second network device is available for a secure communications service is a function of a domain name lookup*" as specified by **claim 14**. Ex. 1003 at ¶¶ 643-649. RFC 2543 thus also shows "*The system of claim 16, wherein the determination that the second network device is available for the secure communications service is a function of the result of a domain name lookup*" as specified by **claim 28**. Ex. 1003 at ¶¶ 643-649.

10. RFC 2543 Anticipates Claim 15 and 30

RFC 2543 anticipates claims 1 and 16, from which claims 15 and 30 depend, respectively. *See* § 1, *above*. RFC 2543 shows that the SIP architecture includes several devices, including: at least two SIP user agents (*e.g.*, software for a SIP client), one or more SIP servers (such as proxy servers or redirection servers), and one or more location servers. Ex. 1003 at ¶¶ 474-475. RFC 2543 shows that each user agent and each proxy server is on a separate device. Ex. 1003 at ¶¶ 474-475, 516-526. RFC 2543 also shows that the proxy servers acted on intercepted messages destined for other entities (*e.g.*, the caller or callee). Ex. 1003 at ¶ 565. RFC 2543 thus shows "*The method of claim 1, wherein intercepting the request occurs within another network device that is separate from the first network device*" as specified by **claim 15**. Ex. 1003 at ¶¶ 650-653. RFC 2543 thus also shows "*The system of claim 16, wherein the one or more servers configured to intercept the request are separate from the first network device*" as specified by claim 30. Ex. 1003 at ¶¶ 650-653.

D. RFC 2543 In View of RFC 1889, RFC 2327 Renders Obvious Claims 1-11, 14-25, and 28-30

1. Independent Claims 1 and 16 Would Have Been Obvious

Patent Owner may contend (i) claims 1 and 16 require all network traffic must be encrypted in a secure communication link, and (ii) that RFC 2543 does not describe a process where all multimedia data streams are encrypted. These

distinctions, even if established, would not render claims 1 or 16 patentable. The process of encrypting session data streams is explained in RFC 2543, but it is explained in more detail in RFC 1889 (Ex. 1013) and RFC 2327 (Ex. 1014). A person of ordinary skill would have read these references together because they are cited in RFC 2543, and RFC 2543 explains that the protocols are designed to be used together. As RFC 2543 explains: "SIP is designed as part of the overall IETF multimedia data and control architecture currently incorporating protocols such as . . . **the real-time transport protocol (RTP) (RFC 1889 [3]) for transporting real-time data** and providing QOS feedback . . ., and **the session description protocol (SDP) (RFC 2327 [6]) for describing multimedia sessions**. Ex. 1012 at 8; *see* Ex. 1003 at ¶ 458. Even if the Board were to conclude both that RFC 2543 does not completely describe the process for encrypting session data and that RFC 2543, RFC 1889, and RFC 2327 cannot be considered as a single disclosure, it would have been obvious to a person of ordinary skill in the art in February 2000 to combine the teachings of these RFCs.

2. Dependent Claims 2-11, 14-15, 17-25, and 28-30 Would Have Been Obvious

RFC 2543 anticipates claims 2-11, 14-15, 17-25, and 28-30 for the reasons set forth in §§ IV.C.1-IV.C.10, *above*.

If Patent Owner contends RFC 2543 does not anticipate the claims because it does not show how to encrypt all network traffic, the combined teachings of RFC

2543, RFC 1889, and RFC 2327 also would have rendered that putative distinction obvious. *See* § 1, above. Because RFC 2543 itself describes systems and processes meeting the requirements of each of claims 2-11, 14-15, 17-25, and 28-30, each of those claims also would have been considered obvious by a person of ordinary skill in February of 2000 based on the combined teachings of RFC 2543, RFC 1889, and RFC 2327 for the reasons in §§ IV.C.1-IV.C.10, *above*.

E. RFC 2543 In View of Mobility Support Using SIP Renders Obvious Claims 8-9 and 22-23

RFC 2543 anticipates claims 8-9 and 22-23 for the reasons set forth in §§ IV.C.5-IV.C.6, *above*. Nevertheless, Patent Owner may contend RFC 2543 does not anticipate these claims for certain reasons. 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 8-9 and 22-23 to have been obvious in February of 2000 based on RFC 2543 in view of Mobility Support Using SIP (Ex. 1015).

Mobility Support Using SIP was a proposed modification to the SIP standard that would enable SIP to support call handoff so mobile devices could switch networks during an active call. The Mobility Support Using SIP modification was proposed by Henning Schulzrinne, Ph.D., one of the authors of the RFC 2543. Based on the guidance in RFC 2543 considered in view of

Mobility Support Using SIP, a person of ordinary skill in the art would have found it obvious to use a mobile phone or other device as a SIP device.

If it is found that RFC 2543 does not describe usage of a mobile device as provided in claims 8 and 22, a person of ordinary skill in February of 2000 would have found it obvious to incorporate a mobile device into the SIP scheme based on the guidance in RFC 2543 and Mobility Support Using SIP. Ex. 1003 at ¶¶ 488-489, 631.

If it is found that RFC 2543 does not describe usage of a notebook computer as provided in claims 9 and 23, I believe a person of ordinary skill in February of 2000 would have found it obvious to incorporate a notebook computer into the SIP scheme based on the guidance in RFC 2543 and Mobility Support Using SIP. Ex. 1003 at ¶¶ 488-489, 635. Mobility Support Using SIP specifically lists a laptop computer as a type of device that can be used in the SIP scheme. Ex. 1003 at ¶ 489.

Because RFC 2543 itself describes systems and processes meeting the requirements of each of claims 8-9 and 22-23, each of those claims also would have been considered obvious by a person of ordinary skill in February of 2000 based on the combined teachings of RFC 2543 and Mobility Support Using SIP for the reasons in §§ C.1 and C.6, *above*.

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 1-11, 14-25, and 28-30 be canceled as unpatentable.

Dated: December 6, 2013

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. 8,504,697

ATTACHMENT A:
PROOF OF SERVICE OF THE PETITION

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of December, 2013, 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: December 6, 2013

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. 8,504,697

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

Exhibit #	Reference Name
1001	U.S Patent No. 8,504,697
1002	File History of U.S Patent No. 8,504,697
1003	Declaration of Michael Allyn Fratto re 8,504,697
1004	Curriculum Vitae of Michael Fratto
1005	Declaration of Chris A. Hopen re ’151
1006	Declaration of James Chester re ’504
1007	Aventail Connect v3.01/2.51 Administrator’s Guide and Aventail ExtraNet Server v3.0 Administrator’s Guide (UNIX and Windows NT) (1996-1999)
1008	U.S. Patent No. 5,898,830 to Wesinger
1009	U.S. Patent No. 6,496,867 to Beser
1010	Kent, S., et al., RFC 2401, “Security Architecture for the Internet Protocol,” November 1998
1011	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
1012	H. Schulzrinne et al., RFC 2543, “SIP: Session Initiation Protocol,” March 1999
1013	Schulzrinne, H., et al., RFC 1889, “RTP: A Transport Protocol for Real-Time Applications,” January 1996
1014	Handley, M., et al., RFC 2327, “SDP: Session Description Protocol,” April 1998
1015	E. Wedlund & H. Schulzrinne, “Mobility Support Using SIP,” WOWMOM ‘99 Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia
1016	Mockapetris, P., RFC 1034, “Domain Names – Concepts and Facilities,” November 1987
1017	Mockapetris, P., RFC 1035, “Domain Names – Implementation and Specification,” November 1987
1018	Srisuresh, P., et al., RFC 2663, “IP Network Address Translator (NAT) Terminology and Considerations,” August 1999
1019	Tittel, E., et al., Windows NT Server 4 for Dummies, Ch. 12, pp. 191-210 (1999)

Exhibit #	Reference Name
1020	Microsoft Press, "Microsoft Windows 98 Resource Kit, The Professional's Companion to Windows 98," Ch. 9, pp. 355-396 and Ch. 19, pp. 849-918 (1998)
1021	Aventail AutoSOCKS v2.1 Administration and User's Guide, 1996-1997
1022	Aventail Connect v3.1/v2.6 Administrator's Guide, 1996-1999
1023	U.S. Patent No. 4,405,829 to Rivest et al.
1024	Ferguson, P. and Huston, G., "What Is a VPN? – Part II," The Internet Protocol Journal, Vol. 1, No. 2 (September, 1998)
1025	Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989
1026	Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997
1027	Socolofsky, T., et al., RFC 1180, "A TCP/IP Tutorial," January 1991
1028	RFC 791, "Internet Protocol – DARPA Internet Program Protocol Specification," September 1981
1029	Rescorla, E., et al., RFC 2660, "The Secure HyperText Transfer Protocol," August 1999
1030	Lloyd, B., et al., RFC 1334, "PPP Authentication Protocols," October 1992
1031	Simpson, W., RFC 1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," August 1996
1032	Dierks, T., et al., RFC 2246, "The TLS Protocol – Version 1.0," January 1999
1033	Simpson, W., RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994
1034	Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996
1035	Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September 1998
1036	Pall, G., RFC 2118, "Microsoft Point-To-Point Compression (MPPC) Protocol," March 1997
1037	Gross, G., et al., RFC 2364, "PPP Over AAL5," July 1998
1038	Townsley, W.M., et al., RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999

Exhibit #	Reference Name
1039	Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993
1040	Adams, C., et al., RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols," March 1999
1041	Bradner, S., RFC 2026, "The Internet Standards Process – Revision 3," October 1996
1042	Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996
1043	Malkin, G., RFC 2453, "RIP Version 2," November 1998
1044	Moy, J., RFC 2328, "OSPF Version 2," April 1998
1045	Memorandum Opinion in VirnetX, Inc. v. Microsoft Corporation, 6:07-CV-80 (7/30/09) (EDTX)
1046	VirnetX's Opening Claim Construction Brief in VirnetX Inc. v. Cisco Systems, Inc., et al., 6:10-CV-417 (11/4/11) (EDTX)
1047	Defendants' Responsive Claim Construction Brief in VirnetX Inc. v. Cisco Systems, Inc., et al., 6:10-CV-417 (12/7/11) (EDTX)
1048	VirnetX's Reply Claim Construction Brief in VirnetX Inc. v. Cisco Systems, Inc., et al. , 6:10-CV-417 (12/19/11) (EDTX)
1049	Memorandum Opinion and Order in VirnetX Inc. v. Cisco Systems, Inc., et al., 6:10-CV-417 (4/25/12) (EDTX)
1050	VirnetX Inc.'s and Science Applications International Corporation's Original Complaint and Summons in VirnetX Inc., et al. v. Apple Inc., 6:12-CV-855 (11/6/2012) (EDTX)
1051	Declaration of Jason Nieh, Ph.D., Inter Partes Reexamination Proceeding, Control No. 95/001,269 (April 15, 2010) (USPTO)
1052	Declaration of Angelos D. Keromytis, Ph.D., Inter Partes Reexamination Proceeding, Control No. 95/001,788 (March 29, 2012) (USPTO)
1053	Declaration of Robert Dunham Short III, Inter Partes Reexamination Proceeding, Control No. 95/001,788 (March 29, 2012) (USPTO)
1054	Application No. 13/049,552, Applicant's Appeal Brief (April 25, 2013)
1055	Office Action in Inter Partes Reexamination - Non-Final Office Action, Control No. 95/001,788, December 29, 2011 (USPTO)
1056	Patent Owner's Response to Office Action of December 29, 2011, Control No. 95/001,788, March 29, 2012 (USPTO)

Exhibit #	Reference Name
1057	Curriculum Vitae of Chris Hopen
1058	"Aventail Ships the First Standards-Based Virtual Private Network Software Solution," PR Newswire, PR Newswire Association LLC, May 2, 1997
1059	Szeto, L., "Aventail delivers highly secure, flexible VPN solution," InfoWorld Media Group, June 23, 1997
1060	"Aventail Introduces the First Extranet-Ready Platform; Aventail Previews its Latest Solution, Aventail ExtraNet Center, at Networld+Interop in Atlanta," PR Newswire, PR Newswire Association LLC, October 12, 1998
1061	"Intranet Applications: Briefs," Network World, October 19, 1998
1062	Curriculum Vitae of James Chester
1063	U.S. Patent No. 6,182,141 to Blum
1064	U.S. Patent No. 6,701,437 to Hoke
1065	U.S. Patent No. 6,557,037 to Provino
1066	WAP Forum, Wireless Application Protocol Architecture Specification (April 30, 1998)
1067	W3C, "World Wide Web Consortium and Wireless Application Protocol Forum Establish Formal Liaison Relationship," December 8, 1999
1068	"Data-Over-Cable Interface Specifications (DOCSIS)", SP-RFII01-970326, 1997
1069	Paul Nikolich, "Cable Modems Deliver Fast 'Net Access," Network World 35 (Mar. 1, 1999)
1070	Jim Duffy, "Cabletron Enters Cable Modem Fray," Network World 23 (Dec. 21, 1998)
1071	Brandt, A., "How It Works: Cable Modems," PC World Article, December 13, 1999
1072	Microsoft Dictionary Fourth Edition, 1999
1073	Ferguson, P. and Huston, G., "What Is a VPN? – Part I," The Internet Protocol Journal, Vol. 1, No. 1 (June 1998)
1074	ITU-T Recommendation H.323 (February 1998)
1075	IBM Session Initiation Protocol (SIP)

Exhibit #	Reference Name
1076	Gulbrandsen, A., et al., RFC 2052, "A DNS RR for specifying the location of services (DNS SRV)," October 1996
1077	U.S. Patent No. 6,430,176 to Christie
1078	U.S. Patent No. 6,930,998 to Sylvain
1079	Shorter Oxford Dictionary, Fifth Edition (2002)
1080	Record of Publication of WOWMOM (Ex. 1015) on ACM Digital Library (available at http://dl.acm.org/citation.cfm?id=313281)