

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

AMAZON.COM, INC., AMAZON.COM, LLC,  
AMAZON WEB SERVICES, INC., BAZAARVOICE, INC.,  
GEARBOX SOFTWARE, LLC,  
INTERNATIONAL BUSINESS MACHINES CORPORATION, and  
SOFTLAYER TECHNOLOGIES, INC.,  
Petitioner,

v.

ZITOVault, LLC,  
Patent Owner.

---

Case IPR2016-00021<sup>1</sup>  
Patent 6,484,257 B1

---

Before JAMESON LEE, MICHAEL W. KIM, and DANIEL N. FISHMAN,  
*Administrative Patent Judges.*

FISHMAN, *Administrative Patent Judge.*

FINAL WRITTEN DECISION  
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

---

<sup>1</sup> Case IPR2016-01025 has been joined with this proceeding.

## I. INTRODUCTION

Amazon.com, Inc., Amazon.com, LLC, Amazon Web Services, Inc., Bazaarvoice, Inc., and Gearbox Software, LLC, filed a Petition (Paper 1, “Pet.”) for *inter partes* review of claims 1, 3–8, and 10 of U.S. Patent No. 6,484,257 B1 (“the ’257 patent”) (Ex. 1001) pursuant to 35 U.S.C. §§ 311–319. Zitovault, LLC (“Patent Owner”) filed a Patent Owner Preliminary Response (Paper 7, “Prelim. Resp.”). On April 15, 2016, based on the record before us at the time, we instituted an *inter partes* review of claims 1, 3, 5–8, and 10 (Paper 8, “Dec.”). We instituted that review on the following challenges to the claims:

| References                          | Basis    | Claims challenged |
|-------------------------------------|----------|-------------------|
| Feinberg <sup>2</sup>               | § 102(e) | 6 and 10          |
| Feinberg and Bhaskaran <sup>3</sup> | § 103(a) | 1, 3, 6, and 10   |
| Feinberg and Molva <sup>4</sup>     | § 103(a) | 5, 7, and 8       |

Dec. 40.

After we instituted that review, on May 10, 2017, International Business Machines Corporation and SoftLayer Technologies, Inc. filed another Petition seeking joinder in this proceeding. Case No. IPR2016-01025, Paper 2. On August 29, 2016, after Patent Owner waived the

---

<sup>2</sup> U.S. Patent No. 6,065,046; issued May 16, 2000. Ex. 1002 (“Feinberg”).

<sup>3</sup> U.S. Patent No. 6,266,355 B1; issued July 24, 2001. Ex. 1003 (“Bhaskaran”).

<sup>4</sup> Refik Molva, et al., *Authentication of Mobile Users*, 8 IEEE Network, 26–34 (March/April 1994). Ex. 1004 (“Molva”).

IPR2016-00021  
IPR2016-01025  
Patent 6,484,257 B1

opportunity to file a Preliminary Response (IPR2016-01025, Paper 6) to that Petition, we instituted review in IPR2016-01025 and ordered that the two cases (IPR2016-00021 and IPR2016-01025) be joined. Paper 23.

All further citations to Papers and Exhibits herein refer to Papers and Exhibits in IPR2016-00021. Furthermore, Amazon.com, Inc., Amazon.com, LLC, Amazon Web Services, Inc., Bazaarvoice, Inc., Gearbox Software, LLC, International Business Machines Corporation, and SoftLayer Technologies, Inc. are hereinafter referred to collectively as “Petitioner.”

Patent Owner filed a Patent Owner Response (Paper 15, “PO Resp.”) and Petitioner filed a Reply (Paper 26, “Pet. Reply”). Petitioner relies on the Declaration of Dr. Aviel D. Rubin (Ex. 1005). Patent Owner relies on the Declaration of Dr. Jonathan Katz (Ex. 2007).

Oral Hearing was conducted on January 12, 2017. The record contains a transcript of the hearing (Paper 39, “Tr.”).

We have jurisdiction under 35 U.S.C. § 6. The evidentiary standard is preponderance of the evidence. *See* 35 U.S.C. § 316(e); *see also* 37 C.F.R. § 42.1(d). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons expressed below, we conclude that Petitioner has not met its burden to show, by a preponderance of the evidence, that claims 1, 3, 5–8, and 10 are unpatentable.

#### *A. The ’257 patent*

According to the ’257 patent, prior architectures for secure communications are not scalable. Ex. 1001, 1:66–67. According to the ’257

patent, prior approaches present problems of poor scalability because a centralized server becomes saturated as demand increases and the addition of special ASICs or hardware to aid in the processing (e.g., encryption/decryption processing) is costly. *See id.* at 3:59–4:32. The '257 patent purports to address this problem of scalability by “a distributed software solution for encryption/decryption which is infinitely scaleable [sic] in the number of simultaneous sessions capable of being processed by a server and in terms of bandwidth between clients and servers.” *Id.* at 4:47–51.

Figure 1 of the '257 patent, reproduced below, shows an exemplary prior art configuration.

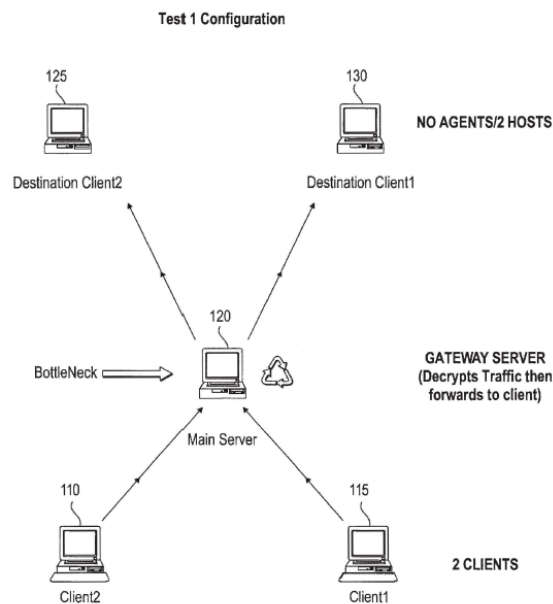


Fig. 1  
(Prior Art)

Figure 1 of the '257 patent, reproduced above, shows two clients 110 and 115 in communication with corresponding destination clients 125 and 130 via main server 120.

In this prior art configuration, main server 120 performs all processing to decrypt the encrypted information received from clients 110 and 115, and forwards the decrypted information to destination clients 125 and 130.

Ex. 1001, 14:35–42. In other words, the sole “agent” for encryption/decryption processing (represented by the triangular arrows) is in main server 120 and, thus, a bottleneck is created at main server 120 in terms of the number of secure sessions between client computers and the processing bandwidth for those sessions.

Figure 2, reproduced below, shows an exemplary system configuration according to the invention.

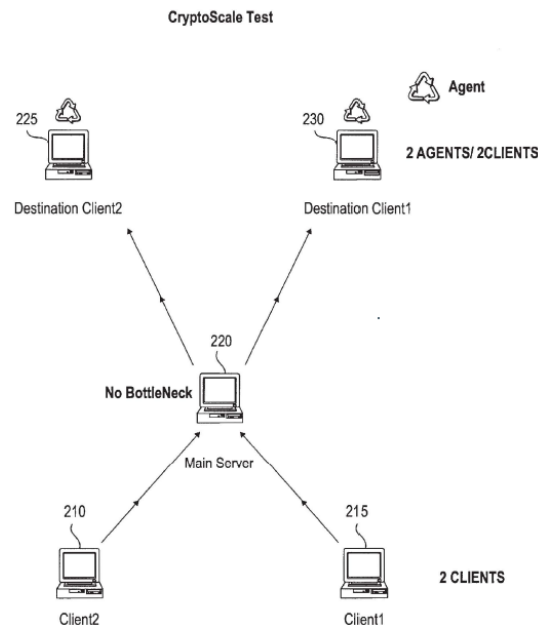


Figure 2 of the '257 patent, reproduced above, shows two clients 210 and 215 in communication with corresponding destination clients 225 and 230 via main server 220.

In this exemplary configuration, main server 220 need not perform all processing to decrypt the encrypted information received from clients 210 and 215, but may, instead, forward the encrypted information to destination clients 225 and 230 in which distributed agents (represented by the triangular arrows) are operable to perform decryption of the received data. *Id.* at 14:55–62.

The exemplary embodiment of Figure 2 distributes the decryption processing (represented by the triangular arrows labeled “agent”) to other computers of the network — specifically agents operable in destination client computers 225 and 230. Thus, main server 220 is no longer responsible for all encryption/decryption processing, and no longer presents a “bottleneck” to the secure communications.

According to the ’257 patent, the invention comprises a main server, agents, and clients. *Id.* at 6:50–51. Processing in these elements is modeled as a finite state machine. *Id.* at 6:62.

Figure 4 of the ’257 patent is reproduced below and shows exemplary operation of such state machine models (described as events processed by the identified entities — main server, agents, and clients):

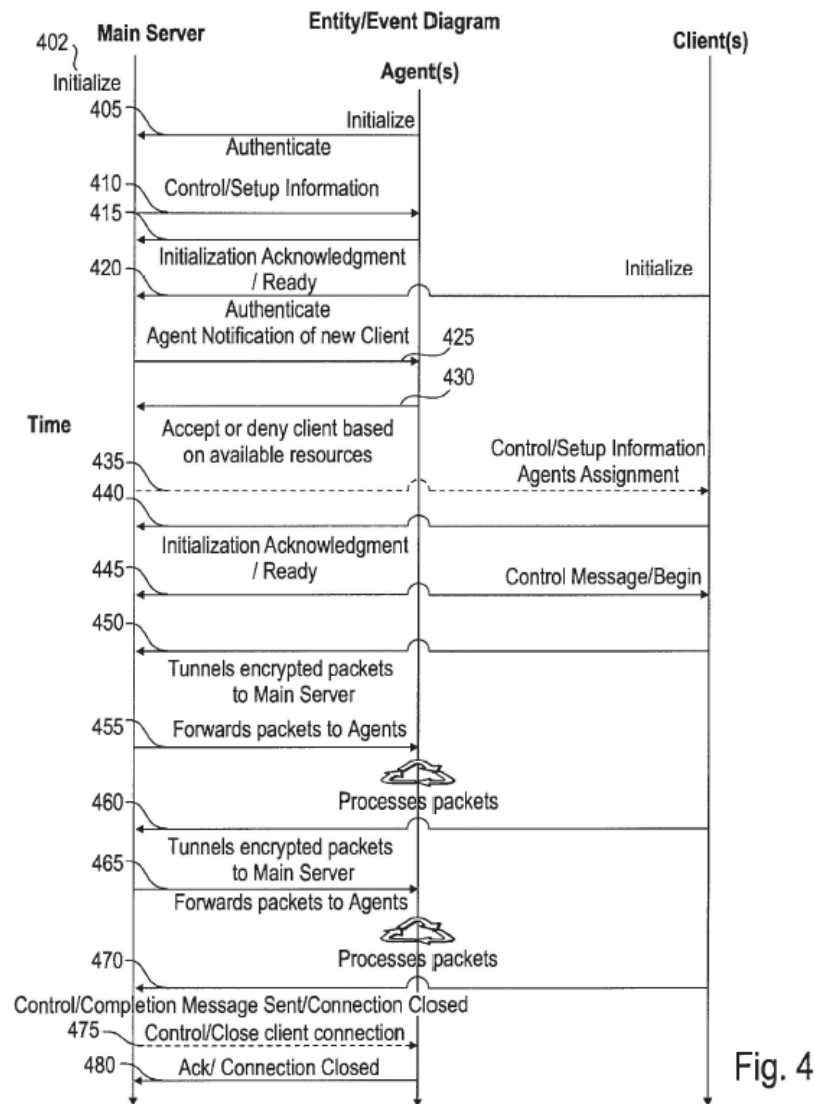


Figure 4 of the '257 patent, reproduced above, shows an exemplary event/entity flow diagram for events processed by the main server, agent, and client entities.

Specifically, Figure 4 shows events 405, 410, and 415 exchanging information between an agent entity and the main server entity to register the agent with the main server. Ex. 1001, 7:19–23. Event 420 represents a client entity attempting to establish a connection with the main server. *Id.* at 7:23–25. If the main server has sufficient bandwidth to service the client's

IPR2016-00021  
IPR2016-01025  
Patent 6,484,257 B1

request, it establishes the connection and processes the client's requests normally (not shown). *Id.* at 7:25–30. If the main server lacks sufficient bandwidth to handle the connection, the main server will unblock (wake up) an agent server to process the connection request. *Id.* at 7:30–34. Thus, the invention purports to distribute the processing required to encrypt/decrypt exchanges between a source and destination device.

### *B. Related Matters*

The parties identify the following related litigation: *ZitoVault, LLC v. Amazon.Com, Inc., Amazon.com, LLC, Amazon Web Services, LLC, Bazaarvoice, Inc. and Gearbox Software LLC*, Western District of Washington, 2:16-cv-00027 (transferred from the Eastern District of Texas, 6:15-cv-00152 (filed March 2, 2015)). Paper 37, 2; Pet. 2. The parties also identify the following related litigation: *ZitoVault, LLC v. International Business Machines Corporation and Softlayer Technologies, Inc.*, Northern District of Texas, 3:16-cv-00962 (transferred from the Eastern District of Texas, 6:15-cv-00906 (filed October 16, 2015)). Paper 37, 2; Case IPR2016-01025, Paper 2, 2.

Patent Owner also identifies a related matter before the Board as: *International Business Machines Corporation and SoftLayer Technologies, Inc. v. Zitovault, LLC*, Case No. IPR2016-01851. Paper 37, 2–3 (institution denied).

### *C. Illustrative Claims*

Independent claims 1 and 6, reproduced below (with some formatting added), are exemplary of the invention:

1. A system for conducting a plurality of cryptographic sessions over a distributed network of computers, employing a distributed automaton running on the network comprising M agents for servicing N number of simultaneous cryptographic sessions wherein bandwidth and number of sessions are scalable by the M agents and latency is potentially reducible to zero comprising:

a main server;

one or more clients communicating over the distributed network with said main server and agents;

M agents communicating with the main server for enlisting additional agents to support incremental cryptographic sessions with the clients to maintain system performance at a desired level; and for encrypting and decrypting communication traffic as it arrives from the clients via the main server, the agents comprising a single-to-many connection (1 client, M agents) with respect to the clients, such that portions of the bandwidth are equally divided among the M agents for processing, and the agents combine the processing power of all computers connected to the system to service encryption and decryption and enable bandwidth to be scalable by the M agents and to reduce latency substantially to zero.

6. A method for implementing a scaleable [sic] software crypto system between a main server and one or more agent servers communicating with one or more clients such that performance of the crypto system is increased to meet any demand comprising

providing a secure communication between the main server, agent server, and one or more clients such that communication between the main server and agent server enlists additional agent servers to support incremental secure sessions in response to maintaining performance at a desired level.

## II. ANALYSIS

### A. *Claim Construction*

In an *inter partes* review, a claim in an unexpired patent shall be given its broadest reasonable construction in light of the specification of the patent in which it appears. 37 C.F.R. § 42.100(b); *see also Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142 (2016) (affirming that USPTO has statutory authority to construe claims according to 37 C.F.R. § 42.100(b)). Under the broadest reasonable construction standard, claim terms are generally given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). “[A] claim construction analysis must begin and remain centered on the claim language itself.” *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004). “Though understanding the claim language may be aided by the explanations contained in the written description, it is important not to import into a claim limitations that are not a part of the claim.” *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004). Furthermore, only those terms that are in controversy need to be construed, and only to the extent

necessary to resolve the controversy. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

Other than the terms discussed below, on the record before us as developed at trial, we determine no other term requires express construction.

*“Session(s)”*

Each of claims 1, 3, 5–8, and 10 recite “session” or “sessions.” Neither the Petition nor Patent Owner’s Preliminary Response (Paper 7; “Prelim. Resp.”) expressly proposed a specific construction of the term “session” or “sessions.” *See generally* Pet. 7–11; Prelim. Resp. 4–7. In our Decision on Institution, we were unable to ascertain any express definition of the term “session” in the Specification of the ’257 patent. Therefore, relying on a standard telecommunications dictionary, we broadly construed the term “session” as “a set of transmitters and receivers, and the data streams that flow between them,” a definition we found consistent with the Specification. Dec. 12–13 (citing Ex. 3002).

Patent Owner argues, in its Response, that the claim language requires “the term session must refer to a connection with a defined beginning and end that can be established for utilizing encryption.” PO Resp. 7. Patent Owner further argues our preliminary interpretation would broadly cover “all communication[s] between any devices connected to a system” and, thus, “[i]f multiple clients attempted to connect to a server simultaneously, all those various connections would constitute only a single ‘session.’” *Id.* at 8. Patent Owner, therefore, contends a “session” must be limited to a “well-defined connection that can be initiated, maintained, monitored, and

destroyed.” *Id.* Patent Owner asserts “[t]he temporal aspect of a session means that a receiver can distinguish packets related to a pre-existing session from packets related to a request for a new session.” *Id.* at 10. Furthermore, Patent Owner contends Dr. Rubin (Petitioner’s expert) agreed with this temporal aspect requirement of a “session.” *Id.* at 10–11 (citing Ex. 1005 ¶ 41).

Petitioner acknowledges “[o]f course a session begins and ends at some point—that is axiomatic.” Pet. Reply 4. However, Petitioner argues the ’257 patent “provides no basis for limiting the claims to a particular process of ‘negotiation,’ ‘initiation,’ or termination.” *Id.* at 2. Petitioner contends any number of events may signify the beginning of a session including, for example, simply commencing the sending of packets. *Id.* (citing Ex. 2006, 17:17–20). Similarly, Petitioner asserts a “session” need not have a pre-defined end, but may simply stop sending data to signify an end of a “session.” *Id.* (citing Ex. 2006, 18:21–22).

We are persuaded that our preliminary interpretation of “session” in our Decision on Institution is, at least in some respect, overly broad. Independent claims 1, 6, 7, and 10 each refer to “sessions” in plural, and independent claim 7 refers to “simultaneous” sessions. Thus, the term “session” must be understood, at least, in such a manner as to allow multiple sessions to be distinguished from one another. Although independent claim 5 does not recite “sessions” in plural, the same term should be construed consistently across all claims. Accordingly, we conclude that there must be sufficient delineation within a proper construction of “session” that separates a “session” between one client and one server and a different “session” when

one of the client and server are replaced, and that separates multiple sessions from each other even between the same pair of client and server. During Oral Hearing there were extensive discussions regarding proper construction of “session.” See Tr. 7:9–22:18, 43:11–65:15, 74:21–76:13. At Oral Hearing, counsel for Petitioner agreed that “session” should be understood as communications having a recognizable beginning and a recognizable end. *Id.* at 10:13–16 (“Of course a session has a beginning and an end. I think that is axiomatic in a session. I think that is how Dr. Rubin defined it in his declaration”); see also *id.* at 12:21–13:5, Ex. 1005 ¶ 41. Patent Owner also agreed that if the construction of session is made to include a recognizable beginning and a recognizable end, that would be a proper construction for the term:

JUDGE LEE: Can you tell me why it wouldn’t be enough to add in the construction with a recognizable beginning and end? If we added that to the preliminary construction, would that still be incorrect according to Patent Owner?

MR. NEMUNAITIS: I think it depends somewhat on what is meant by recognizable beginning and end. As Mr. Kinsel mentioned in his presentation, you know, any communication over the Internet, because of the limits of the physical world, it takes electrons time to communicate information, is going to have some sort of beginning and end that could be detected in some way.

But assuming that’s not what we are talking about when we say recognizable beginning and end, we are talking about a recognition from the endpoints, okay, now we have this connection, now we have this session, now we don’t, then I would agree that would be one way to --

JUDGE LEE: You would agree that that would be al[l]right?

MR. NEMUNAITIS: Yes, with that understanding.

*Id.* at 53:13–54:10.

In view of the further development of this case in trial, we modify our preliminary construction of “session” to add the requirement of a recognizable beginning and a recognizable end of the communication. Such a revision to our construction remedies the problem with our preliminary interpretation, discussed *supra*, that there must be delineation between multiple sessions to allow one to distinguish multiple sessions from one another. However, we note that our modified interpretation is not limited to any particular technique or protocol for recognizing the beginning and end of a session exchanged between a transmitter and a receiver. A wide variety of techniques for such beginning and ending determinations are within the scope of our interpretation of “session,” including SSL and IPsec protocols disclosed in the exemplary embodiments of the ’257 patent. Patent Owner’s counsel agreed that the claims are not limited to particular techniques or protocols for such recognition of the start and end of a session:

JUDGE FISHMAN: Patent Owner’s position is that the claims are broader than the embodiments of the Ellis spec which deal with IPsec and SSL?

MR. NEMUNAITIS: Yes, our position is that the claims are not limited to only the embodiments that use SSL or IPsec. There could be other protocols that could be used.

Tr. 65:10–15.

Therefore, we refine our interpretation of “session,” in the context of the challenged claims, to mean “a set of transmitters and receivers, and the data streams that flow between them wherein each data stream flowing between the transmitters and receivers has a recognizable beginning of the data stream transmission and a recognizable end of the data stream transmission.”

*“Communication Sessions”*

Claim 3 depends from claim 1 and recites, in relevant part, “wherein said system for providing one or more communication sessions . . . comprises . . . .” Claim 4 depends from claim 1 and recites, in relevant part, “wherein the system for establishing communication sessions.” The preamble of claim 1 recites, in relevant part, “[a] system for conducting a plurality of cryptographic sessions . . . comprises . . . .” The term “communication sessions” appears nowhere else in the ’257 patent. Claims 3 and 4 further define the system of claim 1 but the claims, *per se*, do not further define the “communication sessions.” We conclude the “communications sessions” recitation of claims 3 and 4 simply refers to, and has the same meaning as, “cryptographic sessions” recited in claim 1. We interpret “cryptographic sessions” below.

*“Secure Session(s),”  
“Cryptographic Session(s),” “Crypto Sessions,” and  
“Secure Cryptographic Session(s)”*

The claims refer variously to “cryptographic session(s),” “crypto sessions,” “secure session(s),” and “secure cryptographic session(s).” As above, we find no limiting definition of these terms in the Specification of the ’257 patent. “Secure session(s)” and “cryptographic session(s)” appear to be used interchangeably within the Specification of the ’257 patent. “Crypto sessions” and “secure cryptographic session(s)” do not appear in Specification of the ’257 patent but appear only in some claims. Broadly, but reasonably, we determine that all of these terms, in singular form, mean a “session” in which exchanged packets are encrypted, and that all of these terms, in plural form, mean more than one “session” in which exchanged packets are encrypted. *See* Dec. 19. “Session” already has been construed above. It is for these reasons that, although we did not expressly construe “secure session” or “cryptographic session” in our Decision on Institution, the Decision impliedly construes the terms as a “session” (as previously construed) that uses encryption in the exchange of packets. Dec. 19.

Patent Owner argues the implied construction in our Decision on Institution is incorrect (PO Resp. 11) and asserts “[u]nder the proper construction of the term ‘session,’ a secure session requires more than simply the transfer of information that happens to be encrypted” (*id.* at 13). Patent Owner then proposes a hypothetical in which multiple sessions share the same secure key for encryption, suggests such a scenario provides

inadequate security, and further suggests problems that arise in such a shared key scenario. *Id.* Instead, Patent Owner contends a “secure session” must include negotiation for a session key that is specific to that session such that keys are not shared among different sessions. *Id.* at 11–12. Patent Owner further contends Petitioner’s expert agrees that, in the context of the ’257 patent, a “secure session” uses a session key to encrypt communications, and that session keys are unique to a specific session. *Id.* (citing Ex. 2006, 23:2–14, 29:15–19, 143:8–11).

We are not persuaded “secure session” (and the other above-identified terms) should be so narrowly construed. The Specification of the ’257 patent discloses embodiments based on use of SSL and IPsec protocols that, in turn, utilize, for example, the Internet Key Exchange (“IKE”) protocol for key management. *See, e.g.*, Ex. 1001, Fig. 4, 6:2–9:28 (describing the general sequence of establishing a “secure session” utilizing these well-known protocols). Thus, in the context of the ’257 patent Specification, we agree the exemplary embodiments disclose encryption utilizing a session key that is unique to the session and, thereby, establish a “secure session.” However, as discussed *supra*, Patent Owner agrees that the claims of the ’257 patent are not limited to any specific protocols or techniques (such as SSL or IPsec as disclosed in exemplary embodiments). *See* Tr. 65:10–15. Furthermore, the claims do not include a limitation that the encryption key is unique to any particular session. An encryption key that is shared among multiple sessions still provides security for those sessions relative to unencrypted exchanges. It is well established that we do not import

limitations from the specification into the claims. *SuperGuide*, 358 F.3d at 875.

Thus, broadly but reasonably and without improperly importing limitations from the specification into the claims, we interpret “secure session” (and the other various terms identified above in the singular) as “a ‘session’ in which exchanged packets are encrypted.” We further interpret “secure sessions” (and the other various terms identified above in the plural), as “more than one ‘session’ in which exchanged packets are encrypted.”

*B. Claims 6 and 10 Anticipated by Feinberg*

Petitioner asserts independent claims 6 and 10 are anticipated by Feinberg. *See* Pet. 18–26; *see also* Pet. Reply 9–13. To establish anticipation, each and every element in a claim, arranged as recited in the claim, must be found in a single prior art reference. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008); *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001). While the elements must be arranged or combined in the same way as in the claim, “the reference need not satisfy an *ipsissimis verbis* test,” i.e., identity of terminology is not required. *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009); *In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990).

*1. Summary of Feinberg (Ex. 1002)*

Feinberg discloses structures and methods for distribution (storage and transfer) of resources (e.g., computer program modules) between computers on a network. Ex. 1002, Abstract. A user computer in Feinberg

requests download of an identified computer program module from a primary server. *Id.* at 4:17–29. The primary server receiving such a request may determine that it is too busy to provide the requested download and, responsive to that determination, may forward (shunt) the request to a secondary server to process the requested download. *Id.* at 4:30–48.

Feinberg's Figure 1, reproduced below, shows an exemplary environment.

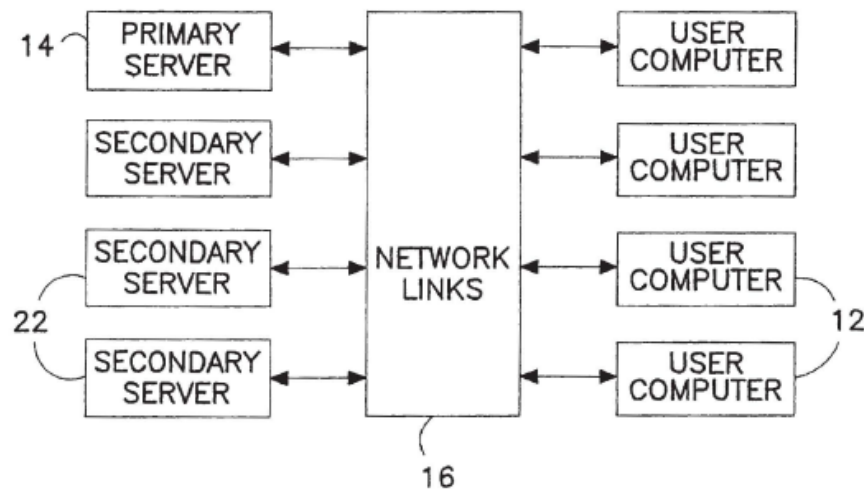


FIG. 1

Feinberg's Figure 1, reproduced above, depicts primary server 14, secondary servers 22, and user computers 12, all coupled to one another through network links 16. Ex. 1002, 10:50–11:8.

A request from a user computer to download a program code module may be encrypted (i.e., stored in the data area of an encrypted packet) and is decrypted by the primary or secondary server responsive to receipt of the

encrypted request. *Id.* at 5:46–53, 8:42–48, 12:25–37. The requested code module is then returned to the requesting user and may be encrypted. *Id.* 11:58–12:13.

## 2. *Analysis of Independent Claims 6 and 10*

Petitioner argues Feinberg discloses a method for implementing cryptographic communications between a main server, one or more agent servers, and one or more clients, as recited in the preamble of claim 6. Pet. 18–21. More specifically, Petitioner contends Feinberg’s user computer 12 (client) includes encryption/decryption unit 60, which is used to encrypt a request to download a code module. *Id.* at 19 (citing Ex. 1002, 12:50–54). Petitioner further contends Feinberg’s primary (main) and secondary (agent) servers each include an encryption/decryption element for decrypting a received request. *Id.* (citing Ex. 1002, 8:41–47, 12:25–35). Petitioner also argues the encryption/decryption elements in each of the servers and the user computers of Feinberg may be implemented as “plug-in encryption code modules,” and that any number of such modules may exist in a system. *Id.* (citing Ex. 1002, 5:28–32). Thus, Petitioner contends, “Feinberg discloses a method for implementing a ‘software crypto system’ [(for secure communications)] between the primary server (‘main server’), secondary servers (‘agent servers’), and user computers (‘clients’).” *Id.* at 19–20. Petitioner further argues Feinberg’s system is scalable (as recited in the preamble of claim 6) because the primary server shunts a request to a secondary server to relieve bandwidth and server load issues and argues any

number of secondary servers may be provided. *Id.* at 20–21 (citing Ex. 1002, 4:43–47).

Petitioner argues Feinberg discloses the recited step of “providing a secure communication.” Pet. 21–23. More specifically, Petitioner contends Feinberg teaches providing secure communication because the “user computers can encrypt requests” (Pet. 21 (citing Ex. 1002, 12:50–56)) and the primary and secondary servers perform encryption and decryption (*id.* (citing Ex. 1002, 12:25–35, 5:50–52)). Petitioner further contends Feinberg discloses the claimed feature “such that communication between the main server and agent server enlists additional agent servers to support incremental secure sessions” because Feinberg’s primary server (main server) forwards/shunts a received request to the least busy secondary server (agent server) when the primary server is overloaded. *Id.* at 21–22 (citing Ex. 1002, 4:34–39, 13:21–23, 17:37–52). Furthermore, Petitioner argues Feinberg discloses that enlisting additional agent servers is responsive to “maintaining performance at a desired level” because Feinberg’s use of secondary servers is “to maintain satisfactory levels of network bandwidth and speed.” *Id.* at 22 (citing Ex. 1002, 9:42–49).

Patent Owner argues “Feinberg does not disclose the use of secure sessions at all” if the term “secure sessions” is properly construed. PO Resp. 23. Specifically, Patent Owner asserts the Petition does not identify what constitutes a “session” in Feinberg or how any such “session is initiated, maintained, or terminated.” *Id.* Patent Owner contends the Petitioner fails to show Feinberg disclosing a “connection with a defined beginning and end.” *Id.* at 24. Patent Owner concludes, “even under the Board’s

preliminary construction [(of “secure sessions”)], Petitioners must demonstrate that Feinberg discloses negotiating the initiation of a stream with a defined beginning and end . . . they have not done so.” *Id.* at 26.

We agree with Patent Owner that Petitioner has failed to identify what constitutes a “session” in Feinberg in accordance with a proper construction of “session.” That proper construction of “session” is set forth above and has been agreed to by the parties. Tr. 10:13–16, 53:13–54:10. We state it again here: “a set of transmitters and receivers, and the data streams that flow between them wherein each data stream flowing between the transmitters and receivers has a recognizable beginning of the data stream transmission and a recognizable end of the data stream transmission.”

Petitioner identifies Feinberg’s disclosure of forwarding (shunting) received requests from the primary server to secondary servers (for purposes of load balancing) teaches the recited “communication between the main server and agent server enlists additional agent servers to support *incremental secure sessions* in response to maintaining performance at a desired level.” Pet. 21–23 (emphasis added). The analysis is excessively generic for the claim recitation of “incremental secure sessions.” It is uncertain what Petitioner regards as a session in Feinberg much less how it begins and how it ends. It is unexplained by Petitioner whether a request in Feinberg begins a session, or something else in Feinberg begins a session. We decline to speculate in that regard. It is Petitioner who bears the burden of proof, and who must account for all the limitations in a claim. In that regard, we note further that it is insufficient for Petitioner to present only dots that may be connected in some unspecified manner to yield the claimed

invention. Instead, Petitioner must make a sufficient connection through the dots to demonstrate a full accounting of the claimed invention.

Petitioner had ample notice of the possibility of a narrower interpretation of “session.” See PO Resp. 7–11, 23–24. Indeed, Petitioner responded to that possibility by referring to its own expert’s testimony that the beginning and end of a session may be signified in a variety of forms. Pet. Reply 2. See *Genzyme Therapeutic Prod. Ltd. P’ship v. Biomarin Pharm. Inc.*, 825 F.3d 1360, 1367 (Fed. Cir. 2016) (“The critical question for compliance with the APA and due process is whether [the parties] received ‘adequate notice of the issues that would be considered, and ultimately resolved, at [the] hearing’”) (internal citation omitted). Nevertheless, Petitioner’s Reply still does not specifically identify a “session” within Feinberg that accounts for what constitutes a session in Feinberg, including when it begins and ends.

Claim 10 recites, in pertinent part, “sharing spare CPU cycles of the computer network for encrypting and decrypting communication to provide N simultaneous secure session[s] among said network of computers.” Petitioner’s analysis with respect to the recitation of “N simultaneous secure session[s]” is deficient for the same reasons we discussed above with respect to the recitation of “incremental secure sessions” in claim 6.

For the above reasons, we are not persuaded Petitioner has established, by a preponderance of the evidence, that claims 6 and 10 are anticipated by Feinberg.

*C. Claims 1, 3, 6, and 10 Obvious Over Feinberg and Bhaskaran*

Independent claim 1 includes a recitation, similar to that of claim 6, that the system supports “incremental secure sessions.” The Petition relies on Feinberg for disclosing such sessions, presenting the same arguments as those it presents for claim 6. *See* Pet. 33–34. Patent Owner argues Feinberg fails to disclose sessions for the same reasons as those that Patent Owner presented with respect to claim 6. *See* PO Resp. 36–37. Petitioner’s Reply asserts essentially the same arguments for claim 1 as it does for claim 6 regarding “incremental secure sessions.” Pet. Reply 17. Petitioner does not rely on Bhaskaran to alleviate the above-identified deficiency in the analysis of Feinberg with respect to claim 6.

The standard for obviousness under 35 U.S.C. § 103(a) is what would have been taught or suggested to the ordinarily skilled artisan with based on the references. The key to supporting any *prima facie* conclusion of obviousness under 35 U.S.C. § 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious and, the Court has noted that, the analysis supporting an obviousness assertion should be made explicit. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007)). A “legal determinations of obviousness, as with such determinations generally, should be based on evidence rather than on mere speculation or conjecture.” *Alza Corp. v. Mylan Labs., Inc.*, 464 F.3d 1286, 1290 (Fed. Cir. 2006). As discussed *supra*, Petitioner failed to account adequately for the recited “sessions.”

Therefore, Petitioner has failed to establish by a preponderance of the evidence that independent claims 1, 6, and 10 would have been obvious over

Feinberg and Bhaskaran and, for the same reasons, has failed to establish claim 3, dependent from claim 1, would have been obvious over Feinberg and Bhaskaran.

*D. Claims 5, 7, and 8 Obvious Over Feinberg and Molva*

Independent claim 5 recites a system that, *inter alia*, is operable to redirect a secure session to another server. Independent claim 7, similar to claims 1 and 6 discussed *supra*, recites enlisting additional agents to support incremental secure sessions. Claim 8 depends from claim 7 and, therefore, incorporates the limitations of its base claim 7.

Regarding independent claim 5, the Petition relies on Molva for disclosing the redirection of a “secure session” to another agent server (Pet. 51–52), but only relies on Feinberg, and not Molva, for disclosing or suggesting a “session.” We acknowledge that, unlike the other independent claims, independent claim 5 only recites “session” in the singular, as opposed to “sessions” in plural. As noted above, however, we construe claim terms consistently across all claims. Accordingly, we conclude that “session” is still properly construed as “a set of transmitters and receivers, and the data streams that flow between them wherein each data stream flowing between the transmitters and receivers has a recognizable beginning of the data stream transmission and a recognizable end of the data stream transmission.”

To that end, there is ambiguity as to Petitioner’s application of the prior art to this combination of references, because Petitioner has not explained sufficiently whether a “redirection” of a “session” is redirection of

the same session, or the end of a first session and the beginning of a second. Petitioner fails to meet its burden on this basis alone.

Ultimately, however, such a distinction is immaterial. If a redirected session is merely a continuation of the same session, Petitioner did not identify adequately where Feinberg or Molva discloses that same session begins and ends. And if a redirected session ends a first session and begins a second session, Petitioner still did not identify adequately where Feinberg or Molva discloses when the first session begins and the second session ends.

Regarding independent claim 7, Petitioner relies only on Feinberg to account for “incremental secure sessions,” and presents the same arguments in that regard as it does for claim 6. As discussed above with respect to independent claim 6, the Petition fails to account adequately for disclosure of “incremental secure sessions” in Feinberg.

Thus, Petitioner has failed to establish by a preponderance of the evidence that claims 5, 7, and 8 would have been obvious over Feinberg and Molva.

#### *E. Motion to Exclude Evidence*

Patent Owner filed a Motion to Exclude certain evidence. Paper 30 (“Mot.”). Petitioner filed an Opposition to Patent Owner’s Motion to Exclude. Paper 32 (“Opp.”). In particular, Patent Owner moves to exclude the entirety of Exhibit 1005 (Dr. Rubin’s Declaration). Mot. 1. According to Patent Owner, Dr. Rubin’s Declaration fails to meet the reliability requirements of 37 C.F.R. § 42.65 because Dr. Rubin “does not disclose the underlying facts or data on which the opinions contained are based as

required by 37 CFR § 42.65(a), given that it does not state the relative evidentiary weight (e.g., substantial evidence versus preponderance of the evidence) used by Dr. Rubin in arriving at his conclusions.” *Id.* at 2.

Furthermore, Patent Owner contends,

Here, the Board cannot assess under FRE 702 whether Dr. Rubin’s opinion testimony is “based on sufficient facts or data,” is “the product of reliable principles and methods,” or if Dr. Rubin “reliably applied the principles and methods to the facts of the case” given that Dr. Rubin did not disclose the standard against which he measured the quantum of evidence in arriving at his opinions.

*Id.* at 3.

Petitioner opposes Patent Owner’s motion, arguing the Board is well-equipped to apply the proper evidentiary standard (here, a preponderance of the evidence) in the final determination of patentability, and further argues the Board has previously held that the statutory evidentiary standard to be applied to the ultimate decision of unpatentability need not be recited or applied by an expert for the expert’s testimony to be accorded weight in the Board’s decision. Opp. 3 (citing *Vibrant Media, Inc. v. General Electric Co.*, Case No. IPR2013-00172, Paper 50, 42).

Initially, we note Patent Owner’s Motion to Exclude fails to identify the portions of Dr. Rubin’s Declaration that allegedly fail to be based upon sufficient facts or data, that allegedly are the product of unreliable principles and methods, or that allegedly fail to reliably apply sound principles and methods to the facts of the case. There is no requirement for an exact or perfect match between the expert’s experience and the field of the patent. *SEB S.A. v. Montgomery Ward & Co., Inc.*, 594 F.3d 1360, 1372–73 (Fed.

Cir. 2010). Thus, Patent Owner fails to meet its burden with respect to this Motion to Exclude. *See* 37 C.F.R. § 42.20(c).

Furthermore, regarding the objections under FRE 702, we note that under 37 C.F.R. § 42.65(a), “[e]xpert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.” Consequently, this objection more properly goes to the weight to be given Dr. Rubin’s testimony, and not to its admissibility.

In any event, Patent Owner’s argument, that Petitioner did not explain the evidentiary weight or standard that was applied by Dr. Rubin, is misplaced. We note that Dr. Rubin is an expert witness, not a fact finder or a tribunal making fact findings. Dr. Rubin need only provide his opinion and, preferably, also provide the underlying reasoning, inclusive of data and facts, in support of his opinion.

For the above reasons, Patent Owner’s Motion to Exclude is *denied*.

#### *F. Conclusion*

Petitioner has failed to show, by a preponderance of the evidence, that any of claims 1, 3, 5–8, and 10 of the ’257 patent are unpatentable.

### III. ORDERS

After due consideration of the record before us, and for the foregoing reasons, it is:

ORDERED that Petitioner has *not* demonstrated by a preponderance of the evidence that any of claims 1, 3, 5–8, and 10 of U.S. Patent No. 6,484,257 B1 patent is unpatentable;

IPR2016-00021  
IPR2016-01025  
Patent 6,484,257 B1

FURTHER ORDERED that Patent Owner's Motion to Exclude Exhibit 1005 is *denied*; and

FURTHER ORDERED that because this is a final written decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2016-00021  
IPR2016-01025  
Patent 6,484,257 B1

PETITIONER:

Amy E. Simpson  
Christina McCullough  
Grant Kinsel  
PERKINS COIE LLP  
[ASimpson@perkinscoie.com](mailto:ASimpson@perkinscoie.com)  
[AmazonZitoVault@perkinscoie.com](mailto:AmazonZitoVault@perkinscoie.com)  
[gkinsel@perkinscoie.com](mailto:gkinsel@perkinscoie.com)

David L. McCombs  
Andrew S. Ehmke  
John Russell Emerson  
Gregory P. Huh  
HAYNES & BOONE, LLP  
[david.mccombs.ipr@haynesboone.com](mailto:david.mccombs.ipr@haynesboone.com)  
[andy.ehmke.ipr@haynesboone.com](mailto:andy.ehmke.ipr@haynesboone.com)  
[russ.emerson.ipr@haynesboone.com](mailto:russ.emerson.ipr@haynesboone.com)  
[gregory.huh.ipr@haynesboone.com](mailto:gregory.huh.ipr@haynesboone.com)

PATENT OWNER:

Michael Casey  
Wayne Helge  
DAVIDSON BERQUIST JACKSON & GOWDEY, LLP  
[ZitoVault\\_IPR@dbjg.com](mailto:ZitoVault_IPR@dbjg.com)  
[whelge@dbjg.com](mailto:whelge@dbjg.com)