Trials@uspto.gov
571-272-7822

Paper No. 12
Date Entered: 8 April 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WOWZA MEDIA SYSTEMS, LLC
and COFFEE CUP PARTNERS, INC.
Petitioner

v.

ADOBE SYSTEMS INCORPORATED
Patent Owner

Case IPR2013-00054 (TLG)
Patent 8,051,287 B2

Before HOWARD B. BLANKENSHIP, THOMAS L. GIANNETTI, and MICHAEL J. FITZPATRICK, *Administrative Patent Judges.*

BLANKENSHIP, *Administrative Patent Judge.*

# DECISION
# DENYING INTER PARTES REVIEW
# 37 C.F.R. § 42.108

## I. BACKGROUND

Petitioner requests *inter partes* review of claims 1-3, 5, 6, 10, 12-14, 16, 17, 21, 23-26, 28, 29, and 33 of the '287 patent under 35 U.S.C. §§ 311 *et seq*. Patent Owner submitted a preliminary response under 37 C.F.R. § 42.107(b) on February 20, 2013. Paper No. 11. We have jurisdiction under 35 U.S.C. § 314.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides as follows:

> THRESHOLD -- The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 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.

For the reasons that follow, the Board, acting on behalf of the Director, denies the petition.

### *A. The '287 Patent (EX 1001)*

The challenged patent relates to establishing an encrypted communication session. Figure 1 of the '287 patent is reproduced below.

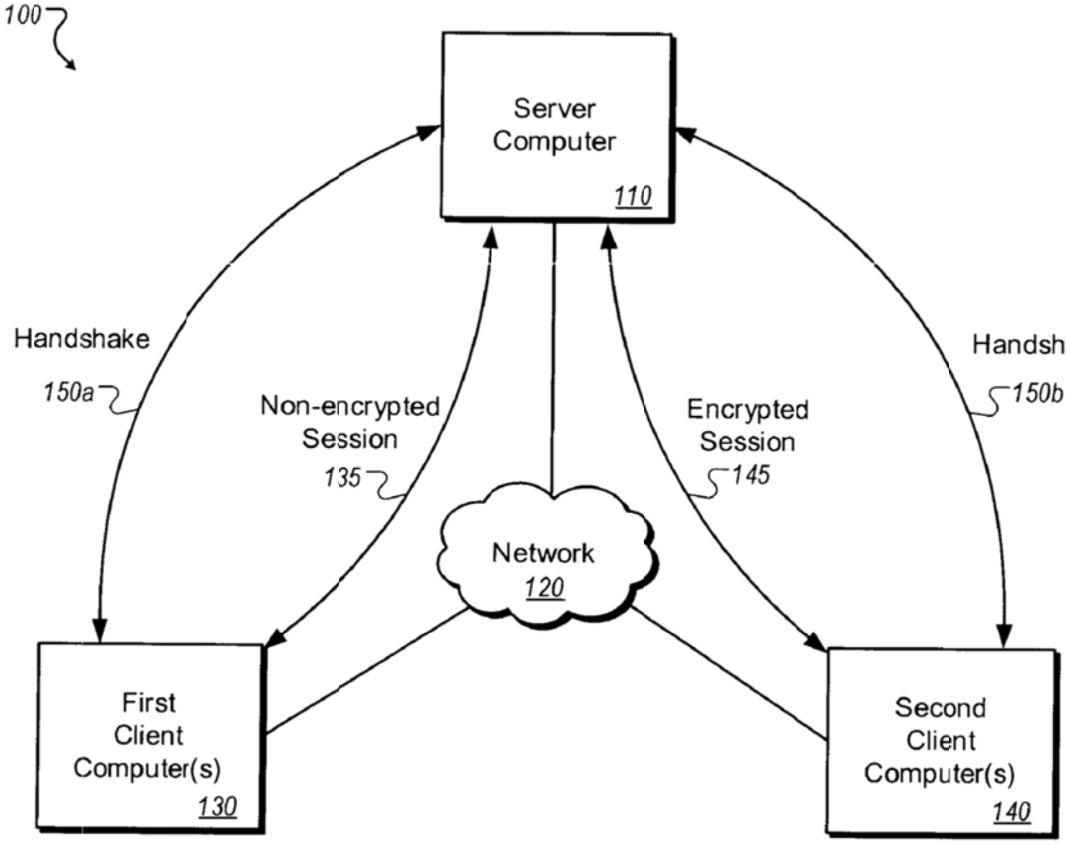


FIG. 1

Figure 1 is said to depict a network environment 100 that includes a server 110 (e.g., a FLASH® Media Server), communicating over a network 120 with a first client computer 130 and a second client computer 140. '287 patent col. 8, ll. 9-15.

Handshakes 150a and 150b precede the sessions 135 and 145 and can include cryptographic information that client 130 may not recognize as such. *Id*. at ll. 15-18. However, the second client computer 140 may include a newer version of software (e.g., a newer FLASH® Player program) that can start an encrypted session 145 with the server computer. *Id*. at ll. 56-59.

Each handshake 150a and 150b may include a block of bytes that contain random data. *Id*. at ll. 25-30. In particular, cryptographic information (e.g., for use in an encryption key establishment protocol) can be included in a previously existing section of the handshake 150 known to contain random bytes, allowing the cryptographic information to be "hidden in plain sight" because the cryptographic information appears to be random. Reverse engineering attempts (i.e., attempts to discover the details of the communication protocol) can thus be handicapped while providing interoperability with existing software. *Id*. at col. 7, l. 67 - col. 8, l. 8; col. 9, ll. 23-46.

### *B. Representative Claim*

Of the challenged claims, claims 1, 10, 12, 21, 23, and 33 are independent. For purposes of this decision, claim 1 is representative. Each of the other independent claims contains the same or substantially similar limitations to those emphasized in claim 1, below. Further, in challenging each of the independent claims, Petitioner relies on the same arguments with respect to the limitations in controversy as represented by claim 1.

> 1. A method comprising:
>
> *establishing, based at least in part on cryptographic information in a pre-defined portion of a handshake network communication, a communication session* to communicate a media stream, *wherein the pre-defined portion of the handshake network communication is reserved for random data*;
>
> receiving through the communication session, as part of the media stream, values of parameters relating to a sub media stream, included in a first header portion of a first real-time, priority-based network communication;

> storing the values of the parameters;
>
> obtaining through the communication session, as part of the media stream, state information included in a control portion of a second real-time, priority-based network communication and a data payload included in the second network communication;
>
> identifying, from the state information, a purpose of the second network communication in relation to the media stream, and whether a second header portion of the second network communication includes one or more new values corresponding to one or more of the parameters;
>
> updating, when the second header portion includes the one or more new values, one or more of the stored values based at least in part on the one or more new values; and
>
> processing the data payload based at least in part on the identified purpose and the stored values of the parameters.

(Emphasis added.)

### *C. Claim Construction*

As a step in our analysis for determining whether to institute a trial, we determine the meaning of the claims. Consistent with the statute and the legislative history of the AIA, the Board will construe the claims using the broadest reasonable interpretation. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48766 (Aug. 14, 2012); 37 CFR § 100(b). The claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). The Office must apply the broadest reasonable meaning to the claim language, taking into account any definitions presented in the specification. *Id*. (citing *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002)).

There is a "heavy presumption" that a claim term carries its ordinary and customary meaning. *CCS Fitness, Inc. v. Brunswick Corp*., 288 F.3d 1359, 1366 (Fed. Cir. 2002). By "ordinary meaning" we refer to *e.g., Biotec Biologische Naturverpackungen GmbH & Co. KG v. Biocorp, Inc.*, 249 F.3d 1341, 1349 (Fed. Cir. 2001) (finding no error in non-construction of "melting"); *Mentor H/S, Inc. v. Med. Device Alliance, Inc.*, 244 F.3d 1365, 1380 (Fed. Cir. 2001) (finding no error in court's refusal to construe "irrigating" and "frictional heat").

Petitioner submits proposed constructions for several terms. Pet. 5-6. However, of the constructions that are proposed by Petitioner, only the phrase "reserved for random data" is material for purposes of this decision. Petitioner submits that rather than its plain and ordinary meaning, "reserved for random data" is to be construed as "[r]eserved for data produced in a manner where there was an equal or approximately equal probability for each possible value." However, Petitioner provides no reasoning or evidence in support of why the phrase should not be interpreted in accordance with its ordinary meaning. Accordingly, we do not adopt Petitioner's special meaning for the claim phrase "reserved for random data."

A claim term that is more pertinent to the issues raised in the Petition and Preliminary Response than those raised by Petitioner is the word "pre-defined" as used in representative claim 1. The '287 patent does not set forth or otherwise indicate any special meaning for the term "pre-defined." The dictionary definition of the transitive verb "predefine" is "to define or determine in advance." *Webster's Third New International Dictionary, Unabridged* (1993). We conclude that this comports with the plain and ordinary meaning, and therefore interpret a "pre-defined" portion of the handshake network communication as a portion of the handshake network communication that is defined or determined in advance.

*D. Related Proceedings*

According to Petitioner, the '287 patent is the subject of a patent infringement lawsuit brought by the assignee (Patent Owner) Adobe Systems Inc., against Wowza, captioned *Adobe Systems Incorporated v. Wowza Media Systems, LLC,* United States District Court, Northern District of California, Case No. CV 11-02243. Pet. 1.

*E. Prior Art*

Petitioner cites the following prior art:

| | | |
|---|---|---|
| Edelman | US 7,272,658 B1 | Sep. 18, 2007 |
| Hellman | US 4,200,770 | Apr. 29, 1980 |
| Bousis | US 2005/0129243 A1 | Jun. 16, 2005 |
| Camp | US 2007/0076877 A1 | Apr. 5, 2007 |

Milan Toth, "*Low level AS3 – Establishing an RTMP connection with Socket and ByteArray,*" *available at* http://www.actionscript.org/resources/articles/630/1/Low-level-AS3---Establishing-an-RTMP-connection-with-Socket-and-ByteArray/Page1.html, June 2007 ("Toth").

Simon Horman, "*SSL and TLS An Overview of a Secure Communication Protocol,*" Security Mini-Conf at Linux.Conf.AU, pp.1-23, Apr.2005 ("Horman").

*1. Edelman (Ex. 1006)*

According to the face of the Edelman patent, the patent is assigned to Patent Owner Adobe Systems Incorporated. Edelman is directed to a real-time priority-based communication system for communicating media streams comprised of multiple media message sub-streams. Edelman col. 3, ll. 6-9.

*2. Toth (Ex. 1008)*

Toth describes reverse engineering an RTMP (Real-Time Messaging Protocol) communication by capturing and analyzing data between a client and server, for the purpose of establishing a connection to an RTMP server with a fake agent and referrer. Toth 1. The first part of the handshake is determined to be a 0x03 byte followed by 1536 random bytes. *Id*. at 3.

*3. Hellman (Ex. 1010)*

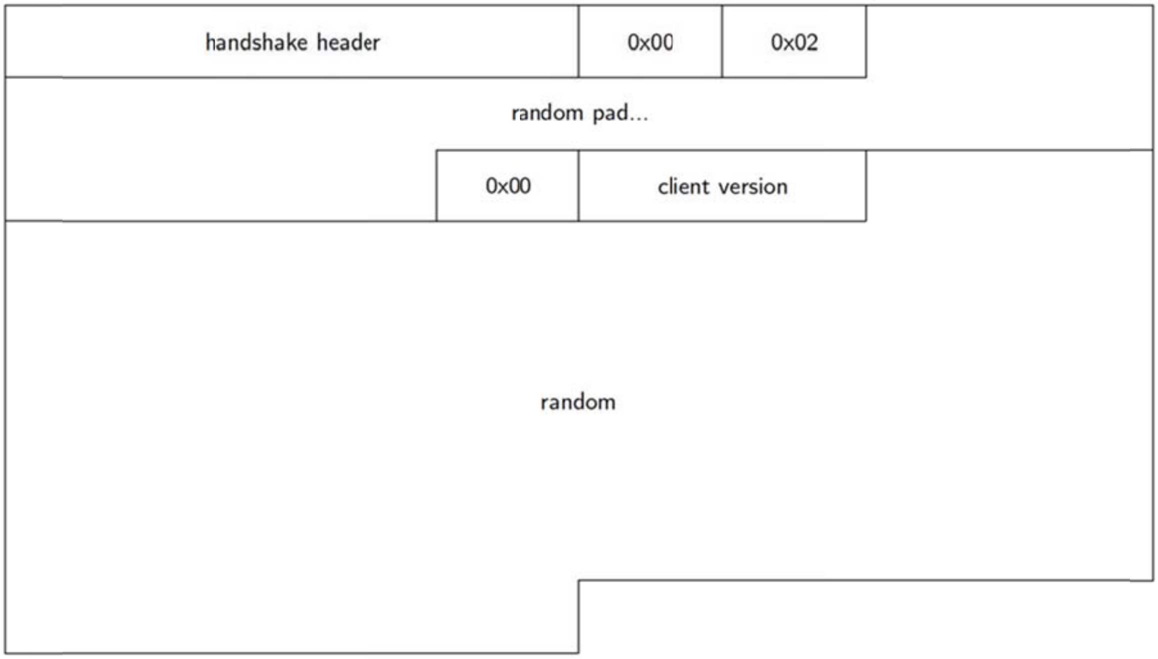
Hellman describes that a generated secure cipher key may be used to encipher and decipher messages transmitted over an insecure communication channel. Hellman col. 2, ll. 14-22.

*4. Horman (Ex. 1011 )*

Horman describes the SSL (Secure Sockets Layer) protocol that makes use of asymmetric encryption for verification and when negotiating a secret key that will be used for symmetric encryption of bulk data transfers. Horman 1 (§ 1.1.1). Horman further describes that in the SSL protocol an RSA[1] client key exchange message consists of the handshake header followed by an encoded pre-master secret that is encrypted using the server's key as sent in the server certificate message. *Id*. at 12.

The unnumbered Figure at page 12 of Horman is reproduced below.

[1] RSA was a well-known Asymmetric Encryption algorithm. *Id*.



RSA Client Key Exchange Message

The Figure depicts an RSA Client Key Exchange Message that consists of a handshake header, 0x00, 0x02, random padding, 0x00, "client version," and "random."

The pre-master secret from the client consists of the maximum version (highest version number) supported by the client followed by 46 random bytes generated by a cryptographic random number generator.[2] The "combined" 48 bytes provide the client's input into the master secret from which the session keys will be derived. *Id*. The (encrypted) pre-master secret is padded to the length of an RSA key by randomly generating pad bytes. *Id*.

[2] There is a minor error in Horman, which refers to a two-byte indication of the maximum version supported by the client "followed by" 48 random bytes. This number 48 appears to be incorrect. According to Petitioner's Exhibit 1012, Alan O. Freier, *The SSL Protocol Version 3.0,* Transport Layer Security Working Group (1996), the client generates a 48-byte pre-master secret from the newest version supported by the client and 46 (not 48) securely-generated random bytes. Freier 28-29.

*5. Bousis (Ex. 1014)*

Bousis describes that an encrypted data-encryption key can be hidden in the random header of a message exchanged between two parties. Bousis Abstract; ¶ [0005]. The random material will be replaced by consecutive bytes from the encrypted random key. ¶ [0021]; Fig. 4.

*6. Camp (Ex. 1015)*

Camp describes (¶ [0056]) that when secure data communication is desired between two terminals, one terminal may generate a keypad by obtaining a random data sequence from a local noise source. The random data sequence constitutes a shared secret known to both terminals, which may be used as the keypad for encrypting and decrypting messages sent between the terminals. ¶ [0053].

An n-bit key sequence K may be extracted from the L-bit random data sequence S (the keypad) as a secret key for encrypting and decrypting transmitted data. ¶ [0069]. A secure, key-encrypted channel can thus be established. ¶ [0013].

*F. Proposed Grounds of Unpatentability*

Petitioner alleges that each of the challenged claims is obvious under § 103(a) over the combination of Edelman, Toth, and Hellman, Bousis, Horman, or Camp. Pet. 5.

Petitioner also alleges that the claims are obvious over various other combinations of references in the alternative, but does not provide support in the Petition for the allegations by applying the combinations as proposed to any of the claims as is required by our rules. For example, Petitioner alleges that "[e]ach of the challenged claims is obvious under § 103(a) over Edelman in view of Toth and further in view of either Hellman or Horman, and further in view of either Bousis or Camp and further in view of any of Cole, Giffin, Lucena, Rowland, and Zander. Pet. 5.

Each Petition must contain "a detailed explanation of the significance of the evidence including material facts. . . ." 37 C.F.R. § 42.22(a)(2). However, this Petition does not explain how the references to be applied in the alternative might remedy deficiencies in the other references, nor applies the references as proposed to be combined in the alternative against any specific claim. In short, Petitioner's alternative allegations fail to "specify where each element of the claim is found . . . ." 37 C.F.R. § 42.104(b)(4). "The Board may exclude or give no weight to the evidence where a party has failed to state its relevance or to identify specific portions of the evidence that support the challenge." *Id*. § 42.104(b)(5).

Of the above-mentioned references, Petitioner cites Raike (Ex. 1016) as a "Cryptography Reference[]" and the following references (Ex. 1017-1021) as "Information Hiding References": Cole, Giffin, Lucena, Rowland, and Zander. Pet. 30; 45-46. As Petitioner provides insufficient analysis of these references as applied to the specific limitations of the claims, we do not consider these references further. *See* discussion *supra*; 37 C.F.R. §§ 42.104(b)(4), (b)(5).

## II. ANALYSIS

### *A. The Petition*

Initially, we note that the Petition's claim chart, to the extent directed to the first step of representative claim 1, which represents the material not taught by Edelman alone, simply refers to "Section VIII.A." Pet. 46. Section VIII.A spans over 16 pages of the Petition. This is significant because this portion of the claim contains the recitation "cryptographic information in a predefined portion of a handshake network" challenged by the Patent Owner in responding to the Petition. Prelim. Resp. 14-25. In that 16-page section, Petitioner offers four different references to be combined in the alternative with Edelman and Toth -- Hellman, Horman, Bousis, and Camp. However, that discussion referenced by the claim chart, while lengthy, provides little or no guidance as to where the challenged recitation is found in these references.

The Petition's claim chart also refers to the entire Sherman Declaration (Ex. 1002; Declaration of Dr. Alan T. Sherman) in general. The Declaration is 100 pages in length and appears, for the most part, simply to track and repeat the arguments for unpatentability presented in the Petition. The lengthy Sherman Declaration is therefore no more helpful that the Petition in determining where the challenged recitation is found in the references. Thus, as the Petition refers only to the Declaration in general, and not to any specific testimony set forth in the Declaration that may relate to specific claim limitations, we have not found the Declaration helpful as support for Petitioner's assertions. *See* Pet. 35, 38, 41, 44 (referring to Sherman Decl. § III.B, entitled "Guidance from *KSR*"). *Cf*. 37 C.F.R. § 42.104(b)(4); 37 C.F.R. § 42.65(a).

### *B. Difference Between the Challenged Claims and the Teachings of Edelman and Toth*

Petitioner submits that there is only one difference between the existing RTMP protocol and the challenged claims:

> The only difference between the invention claimed in the '287 patent and Adobe's preexisting RTMP communications, as set forth in Toth and Edelman, is the requirement that cryptographic information be inserted *in the random data section* of the existing RTMP

> handshake (or some other preexisting portion of a network handshake communication reserved for random data) and that that information be used for encrypting and decrypting the communication.

Pet 9-10 (emphasis added).

Patent Owner in the Preliminary Response does not challenge the substance of Petitioner's statement. For purposes of this decision we will presume, therefore, that the difference between representative claim 1 and the other challenged claims and the combined teachings of Edelman and Toth is substantially as set forth by Petitioner.

Consistently throughout, the Petition refers to the claims as calling for placing the cryptographic information in a "preexisting" portion of the handshake communication. *See, e.g.*, Pet. at each of pages 9, 19, and 31-45. The Petition refers to the "pre-defined" portion of the communication only when directly quoting the claims. *See* Pet. 46-58 (claim chart). We observe, however, that the claims uniformly call for placing cryptographic information in a "pre-defined" portion of a handshake network communication, rather than a "preexisting" portion as indicated by Petitioner. We do not accept this substitution by Petitioner, as it affects the meaning of the claim. "Preexist" is a transitive verb that means "to exist before (something) >>monuments that *preexist* written history<<." *Webster's Third New International Dictionary, Unabridged* (1993). As we have noted *supra* (§ I.C), the ordinary meaning of a "pre-defined" portion of a handshake network communication is a portion of the communication that is defined or determined in advance. Petitioner's substitution, which we reject, would thus render the claims broader in scope when compared to their scope under a proper interpretation of the recited claim language.

*C. Obviousness of the Challenged Claims over Edelman, Toth, and Hellman*

With respect to Hellman, Petitioner cites column 2 of the reference, with its description of generating a secure cipher key that is used to encipher and decipher messages transmitted over an insecure communication channel. Pet. 33-34; *see also Hellman*, § I.E.3 *supra*. Petitioner concludes that it would have been obvious, in light of Hellman, to "establish an encrypted RTMP session by inserting cryptographic information in the preexisting random data section of the RTMP handshake. . . ." Pet. 34.

Petitioner continues, citing the Supreme Court's decision in *KSR*:

> Combining the RTMP References and Hellman "only unites old elements with no change in their respective functions"; is just a "combination of familiar elements according to known methods [with] no more than predictable results"; "simply arranges old elements with each performing the same function it had been known to perform before" and "yields no more than one would expect." *KSR* [*KSR Int'l Co. v. Teleflex, Inc*., 550 U.S. 398 (2007)], 550 U.S. at 416-17. Also, design incentives and other market forces would prompt this predictable variation of RTMP. *See id*. at 417. Also, the teachings of the references described above, as well as design considerations and the demands known in the marketplace would prompt a person of ordinary skill to modify RTMP, as set forth in the RTMP References, when combined with Hellman in the fashion claimed. Doing so would have eliminated the need for additional handshake messages — which slow the process and expend processing power — and would have the additional benefit of obfuscating the cryptographic information, all of which were known design objectives and goals for computer systems and encryption systems.

Pet. 34-35.

We do not agree with Petitioner's obviousness analysis based on *KSR*. In our view, Petitioner has failed to establish certain prerequisites for demonstrating prima facie obviousness under *KSR*. As noted by the Federal Circuit, *KSR* does not authorize conclusory results.

> Although the obviousness analysis should "take account of the inferences and creative steps that a person of ordinary skill in the art would employ," the Supreme Court emphasized that this evidentiary flexibility does not relax the requirement that, "[t]o facilitate review, this analysis should be made explicit." *Id*. [*KSR*] at 418, 127 S.Ct. 1727 (citing [*In re*] *Kahn*, 441 F.3d [977] at 988 ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.")).

*Perfect Web Technologies, Inc. v. InfoUSA, Inc*., 587 F.3d 1324, 1330 (Fed. Cir. 2009). Following the same approach that was rejected by *KSR*, Petitioner's challenge of the claims over Edelman, Toth, and Horman provides mere conclusory statements in support of the legal conclusion of obviousness. Petitioner does not identify any teaching in the applied prior art of establishing an encrypted RTMP session by inserting cryptographic information in a preexisting random data section of the RTMP handshake. Further, Petitioner offers no convincing rationale, in light of the teachings of the prior art, with respect to why one of ordinary skill in the art would have chosen to establish an encrypted RTMP session by inserting cryptographic information in a pre-defined portion of the RTMP handshake reserved for random data. As required by 37 C.F.R. § 42.104(b)(4), a Petition must specify where each element of a challenged claim is found in the prior art patents or printed publications. *See* discussion *supra*. Petitioner has failed to do so.

*D. Obviousness of the Challenged Claims over Edelman, Toth, and Horman*

Petitioner submits that Horman teaches "inserting cryptographic information into network communications in a *preexisting* portion of the communication containing random data. . . ." Pet. 35 (emphasis added). In particular, Petitioner points to Horman's disclosure of an RSA Client Key Exchange Message (*Horman,* § I.E.4 *supra*). Pet. 36-37. "[D]uring the Client Key Exchange step of the SSL/TLS handshake process, cryptographic information is inserted into a preexisting field of the handshake communication that is padded with random PKCS padding. . . ." *Id*. at 36.

Petitioner notes, correctly, that in Horman the "pre-master secret is used to generate a cryptographic key." Pet. 37. From the description in Horman of inserting cryptographic information "into a preexisting field" of a handshake communication that is padded with random data, Petitioner concludes that it would have been obvious, in light of Horman, to "establish an encrypted RTMP session by inserting cryptographic information in the preexisting random data section of the RTMP handshake. . . ." *Id*. Petitioner relies on *KSR* as support for obviousness insofar as *KSR* discusses uniting old elements with no change in respective functions, combining familiar elements according to known methods with predictable results, and design incentives and other market forces. *Id.* at *38*.

However, *KSR* is not apposite, because Petitioner does not identify any teaching in Horman or any of the other applied prior art of establishing an encrypted RTMP session by inserting cryptographic information in a preexisting random data section of the RTMP handshake. Further, Petitioner does not identify the "preexisting field" in Horman into which cryptographic information is alleged to be inserted.

We have reviewed Horman and Petitioner has not identified any suggestion in the reference of inserting cryptographic information into a *pre-defined* (as opposed to preexisting) random data field. Horman describes inserting cryptographic information -- a pre-master secret that consists of an encrypted version of the client version and randomly generated bytes -- into the fields reserved for the cryptographic information, labeled "client version" and "random." *See Horman*; § I.E.4 *supra*. But this is not a pre-defined random data field because it does not contain random data. Harmon does describe that randomly generated pad bytes ("random pad. . .") are added to the message to render the Exchange Message the proper length of the RSA key. However, this "padding" of the message length is not the same as inserting cryptographic information in a *pre-defined* portion of the communication containing random data, as the claims require.

Further, Petitioner offers no convincing rationale, in light of the teachings of the prior art, with respect to why one of ordinary skill in the art would have chosen to establish an encrypted RTMP session by inserting cryptographic information in a pre-defined portion of the RTMP handshake that is reserved for random data.

The Petition must specify where each element of a challenged claim is found in the prior art patents or printed publications. Petitioner has failed to do so. 37 C.F.R. § 42.104(b)(2).

### *E. Obviousness of the Challenged Claims over Edelman, Toth, and Bousis*

Bousis describes that an encrypted data-encryption key can be hidden in the random header of a message exchanged between two parties. Bousis Abstract; ¶ [0005]. However, the term "header" in Bousis does not refer to a conventional message header. As pointed out by Patent Owner, Bousis teaches that "the header principle should not be construed to represent a header according to some pre-existent standard for transmission or storage. In this context, the header simply means some part 'at or near the beginning of the data exchange'." ¶ [0005].

As shown in Figure 3, Bousis describes writing data that is encrypted with a randomly generated key into a file, encrypting the randomly generated key with a shared secret key, hiding the encrypted random key in the encrypted data file, and finally transferring all the data for retrieval and decryption using the shared secret key and the retrieved random key. Bousis ¶¶ [0018]-[0019]. The encrypted data and the encrypted random key may thus be placed into the same file. ¶ [0020]. A number (Nh) of bytes of random material may be placed at the beginning of the file, appending Nd bytes of encrypted data after the Nh bytes. *Id*.; Fig. 4.

Bousis also describes hiding the encrypted key. A shared function F that is known by both the transmitting and receiving systems can be used to return a selection Nr bytes from the Nh bytes[3] of random material. For each of the returned bytes, the random material will be replaced by consecutive bytes from the encrypted random key. Bousis ¶ [0021]; Fig. 4. By distributing the bytes of the encrypted random key over a pool of random material, and appending to this the encrypted material itself, a cryptanalyst cannot know which bytes in the transmitted data belong to the random material, to the encrypted data, and to the encrypted random key. ¶ [0028].

As recognized by Petitioner (Pet. 39), however, Bousis does not disclose inserting cryptographic information in a preexisting handshake communication. Petitioner asserts that in light of Bousis, it would have been obvious to "establish an encrypted RTMP session by inserting cryptographic information in the

[3] Bousis contains a typographical error in paragraph [0021], where "Nb" should be "Nh."

preexisting random data section of the RTMP handshake. . . ." *Id*. at 40. Petitioner once again relies on *KSR*, for substantially the same principles as previously. *See supra*. But Petitioner does not identify any teaching or suggestion in Edelman, Toth, or Bousis with respect to establishing an encrypted RTMP session, much less establishing such a session by inserting cryptographic information in a pre-defined portion of an RTMP handshake that is reserved for random data.

Further, Petitioner offers no convincing rationale, in light of the teachings of the prior art, with respect to why one of ordinary skill in the art would have chosen to establish an encrypted RTMP session by inserting cryptographic information specifically in a pre-defined portion of the handshake that is reserved for random data. Accordingly, we find insufficient support for the Petitioner's conclusion that "a person of ordinary skill would have known that inserting cryptographic information in a handshake is simply a predictable combination" of Edelman, Toth, and Bousis. Pet. 39.

### *F. Obviousness of the Challenged Claims over Edelman, Toth, and Camp*

Petitioner cites portions of Camp (*see Camp*, § I.E.6 *supra*), and concludes, without explanation, that it would have been obvious in light of Camp to establish an encrypted RTMP session by inserting cryptographic information in the preexisting random data section of the RTMP handshake. Pet. 43. Petitioner also cites *KSR*. *Id*. at 43-44.

But as noted *supra*, Petitioner does not identify any teaching in Edelman, Toth, or Camp of establishing an encrypted RTMP session by inserting cryptographic information in a preexisting random data section of the RTMP handshake. Further, as noted *supra*, Petitioner offers no convincing rationale, in light of the teachings of the prior art, with respect to why one of ordinary skill in the art would have chosen to establish an encrypted RTMP session by inserting cryptographic information in a pre-defined portion of the RTMP handshake that is reserved for random data.

## III. CONCLUSION

The Petition does not persuade us that there is a reasonable likelihood that at least one of the challenged claims is unpatentable based on the asserted grounds. We therefore deny the petition for *inter partes* review and decline to institute trial on any of the asserted grounds as to any of the challenged claims. 37 C.F.R. § 42.108.

## IV. ORDER

In consideration of the foregoing, it is hereby

**ORDERED** that the petition is denied as to all challenged claims and no trial is instituted.

For Patent Owner:

Lissi Mojica
Kevin Greenleaf
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
Lmojica@slwip.com
Kgreenleaf@slwip.com

For Petitioner:

Barry F. Irwin
Brent Ray
KIRKLAND & ELLIS, LLP
barry.irwin@kirkland.com
brent.ray@kirkland.com