

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC and
LENOVO (UNITED STATES) INC.,
Petitioners,

v.

ERICSSON AB,
Patent Owner.

IPR2025-00004
Patent 11,122,313 B2

Before GEORGIANNA W. BRADEN, NORMAN H. BEAMER, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Google LLC and Lenovo (United States) Inc. (collectively “Petitioner”) filed a Petition (Paper 3, “Pet.”) requesting *inter partes* review of claims 1–7, 9, 11–17, and 19 of U.S. Patent No. 11,122,313 B2 (Ex. 1001, “the ’313 patent”). Ericsson AB (“Patent Owner”) filed a Preliminary Response (Paper 11, “Prelim. Resp.”).

Under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.4(a), we have authority to determine whether to institute review. Based on the current record and for the reasons explained below, Petitioner has shown that there is a reasonable likelihood that it would prevail with respect to at least one of the challenged claims. Therefore, pursuant to § 314, we institute an *inter partes* review of claims 1–7, 9, 11–17, and 19 in the ’313 patent on all challenges included in the Petition.

A. *Real Parties in Interest*

Petitioner identifies Google LLC and Lenovo (United States) Inc. as the real parties-in-interest. Pet. 4. Petitioner also identifies Lenovo (Beijing) Co., Limited, Lenovo Group Ltd., Lenovo Information Products Shenzhen Co. Ltd., Lenovo PC HK Limited, Lenovo (Shanghai) Electronics Technology Co. Ltd., Motorola Mobility LLC, and Motorola (Wuhan) Mobility Technologies Communication Co., Ltd. as having been accused of infringement in the pending related matters in the U.S. District Court for the Eastern District of North Carolina and the International Trade Commission, while asserting that “Petitioners do not believe that these defendants are Real Parties-in-Interest.” *Id.*

Patent Owner identifies Ericsson AB, Ericsson Inc., and Telefonaktiebolaget LM Ericsson as the real parties-in-interest. Paper 4 (Patent Owner’s Mandatory Notices), 1.

B. Related Matters

The parties indicate that the '313 patent has been asserted in the following district court litigation: *Telefonaktiebolaget LM Ericsson et al. v. Lenovo (United States), Inc. et al.*, Case No. 5:23-cv-00570 (E.D.N.C.). Pet. 5; Paper 4, 2. The parties also indicate that the '313 patent has been asserted in the following International Trade Commission proceeding: *Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same*, Inv. No. 337-TA-1376 (I.T.C.). Pet. 6; Paper 4, 2.

The parties indicate that the application from which the '313 patent issued is related to, *inter alia*, an application from which U.S. Patent No. 9,313,178 (“the '178 patent”) issued. Pet. 4–5; Paper 4, 1. Petitioner indicates that, concurrently with this Petition, Petitioner filed a petition for *inter partes* review of the '178 patent in IPR2025-00003. Pet. 5; *see* Paper 4, 2.

C. The '313 patent

The '313 patent is titled “Method and System for Secure Over-the-Top Live Video Delivery” and it issued on September 14, 2021. Ex. 1001, codes (45), (54). It is a continuation of a U.S. patent application and claims priority to several other continuation applications, as well as a provisional application, the earliest of which was filed on June 23, 2011. *Id.* at codes (60), (63).

1. Written Description

The '313 patent relates to methods and apparatus for managing the distribution and use of a plurality of content encryption keys for use in the protection of live streaming content. Ex. 1001, 1:51–53. According to the '313 patent, “[f]or live streaming content with long or indefinite

durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised.” *Id.* at 1:30–33. The ’313 patent discloses “generating a series of content encryption keys and providing them serially to a packaging server for encrypting a content item, wherein each content encryption key is provided upon expiration of a period of use of a serially preceding content encryption key.” *Id.* at 1:53–58. The ’313 patent refers to the transitioning between use of different keys as key “rotation.” *Id.* at 2:4–6.

One embodiment of the ’313 patent is illustrated in Figure 1, which is reproduced below:

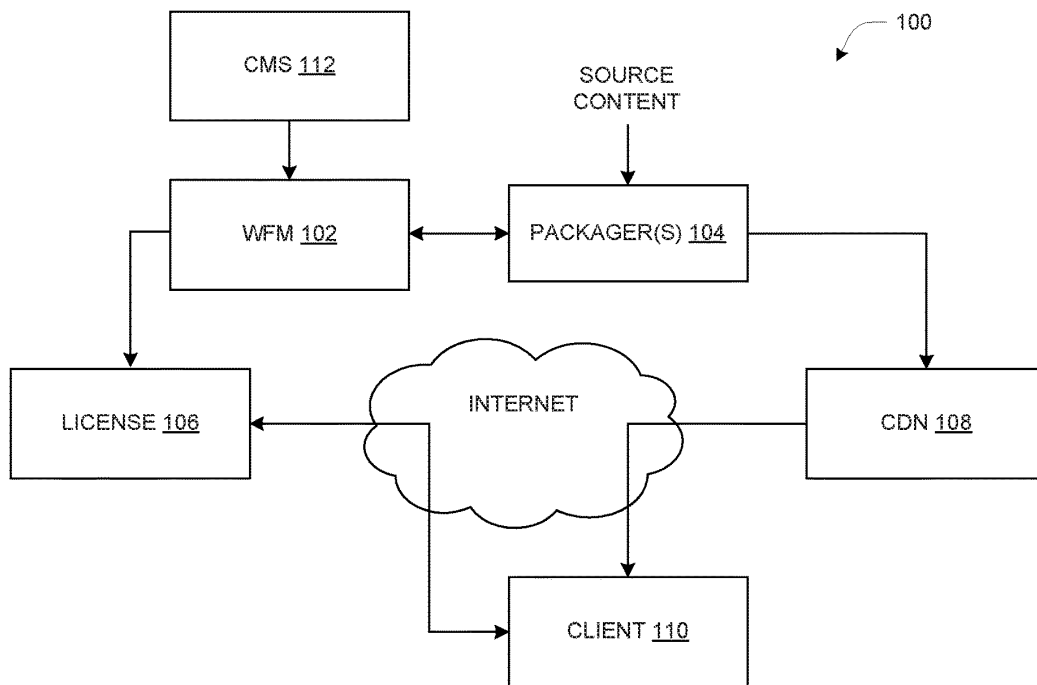


Fig. 1

Figure 1 of the ’313 patent, above, is a box diagram depicting content delivery system 100, including “workflow manager (WFM) 102, one or more packaging servers or ‘packager(s)’ 104, a license server 106, a content

delivery network (CDN) 108, client devices or ‘clients’ 110, and a content management system (CMS) 112.” Ex. 1001, 4:48, 5:14–19. According to the ’313 patent, “packager(s) 104 receive source content and process or ‘package’ the source content so that it may be delivered to the clients 110 via the CDN 108.” *Id.* at 5:19–22. The ’313 patent explains that “packager(s) 104 perform content encryption using a series of content encryption keys.” *Id.* at 5:22–24.

The ’313 patent discloses that packager 104 acquires content encryption keys from workflow manager (WFM) 102. Ex. 1001, 5:55–57. According to the ’313 patent, “WFM 102 generates an initial content encryption key and assigns it a content encryption key identifier.” *Id.* at 6:1–2; *see also id.* at 3:38–40 (“Each content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier.”). For example, in one embodiment, “the content encryption key identifier is initially set to zero and all future content encryption key identifiers are based on a relative offset to the initial content encryption key identifier.” *Id.* at 6:2–6; *see also id.* at 6:6–14 (describing other examples of content encryption key identifiers).

The ’313 patent describes WFM 102 as “provid[ing] the initial content encryption key and lifespan of the key to the packager 104,” which then “encrypts the content using the initial content encryption key until it expires.” Ex. 1001, 6:21–25. According to the ’313 patent, “[t]he new content encryption key is made available by the WFM 102 to the packager 104 before the previous content encryption key has expired to allow for uninterrupted encryption.” *Id.* at 6:40–43. The ’313 patent also describes that “[i]f the current content encryption key needs to be expired,

... the key is ‘rotated’, i.e., the current content encryption key is expired and a new one is put into use.” *Id.* at 11:28–31.

The ’313 patent discloses that “[e]ncrypted content is uploaded by the packager 104 to a content delivery network (CDN) 108, from which it may be retrieved by clients 110.” Ex. 1001, 6:49–51. To decrypt the encrypted content, clients 110 must first obtain the content encryption keys from license server 106. *Id.* at 6:52–55. In one embodiment, the ’313 patent describes license server 106 as storing “the content encryption key, content encryption key identifier, content encryption key lifespan (or expiration), and the location of the encrypted content.” *Id.* at 6:65–7:1.

According to the ’313 patent,

During ongoing retrieval of content, the client device detects content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content, issues requests to the license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached, and applies the second key for content decryption after the key rotation boundary is reached.

Ex. 1001, 2:30–38. In one embodiment, the ’313 patent describes that “packager 104 notifies the client 110 of the key change by updating a manifest file that describes the encrypted content with a flag that describes the expiration of the previous key.” *Id.* at 7:65–8:3.

2. *Illustrative Claim*

As noted previously, Petitioner challenges claims 1–7, 9, 11–17, and 19. Pet. 1. Claims 1 and 11 are independent claims. Claim 1 is representative of the challenged subject matter and is reproduced below with Petitioner’s identifiers in brackets, which do not impact our analysis (*see Id.* at ix–xii, Claim Listing):

1. [1PRE] A method for handling secure distribution of live video content comprising:

[1A] sending a request for live media playback;

receiving a live media playback request response, [1B] the live media playback request response comprising content encryption keys and content encryption key identifiers;

[1C1] receiving encrypted live media content and manifest files from a content delivery server, [1C2] wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content;

[1D] applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary;

[1E] prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

[1F] applying the second content encryption key for content decryption after the key rotation boundary is reached.

Ex. 1001, 12:23–44.

D. Asserted Challenges to Patentability and Evidence of Record

Petitioner challenges the patentability of claims 1–7, 9, 11–17, and 19 of the '313 patent based on the following reference or combination of references:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–4, 6, 7, 11–14, 16, 17	103	Peterka ¹
1–4, 6, 7, 11–14, 16, 17	103	Peterka, Suzuki ²
1–4, 6, 7, 9, 11–14, 16, 17, 19	103	Peterka, Bocharov ³
1–4, 6, 7, 9, 11–14, 16, 17, 19	103	Peterka, Suzuki, Bocharov
5, 15	103	Peterka, Bocharov, Peterka308 ⁴ , Chen ⁵

Pet. 7. In support of its patentability challenge, Petitioner relies on, *inter alia*, the Declaration of Anthony J. Wechselberger (“Mr. Wechselberger”).

Ex. 1003. Patent Owner contests the challenges to patentability. *See* Prelim. Resp. 1, 7–20.

II. PRELIMINARY MATTER

A. Claim Construction

A claim “shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b).” 37 C.F.R. § 42.100(b). Under that standard, the “words of a claim ‘are generally given their ordinary and customary meaning.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).

¹ U.S. Patent Application Publication No. 2002/0172368 A1, published Nov. 21, 2002 (Ex. 1005) (“Peterka”).

² Japanese Unexamined Patent Application Publication No. 2004-166153, published June 10, 2004, filed Nov. 15, 2002 (English translation, Ex. 1006) (“Suzuki”).

³ U.S. Patent Application Publication No. 2010/0235528 A1, published Sept. 16, 2010 (Ex. 1007) (“Bocharov”).

⁴ U.S. Patent Application Publication No. 2008/0270308 A1, published Oct. 30, 2008 (Ex. 1008) (“Peterka308”).

⁵ European Patent Application Publication No. 1 418 756 A2, published May 12, 2004, filed Oct. 29, 2003 (Ex. 1009) (“Chen”).

Petitioner contends “[n]o claim term requires that the Board adopt an exact outer boundary construction because the prior art relied upon herein meets the claims under any plausible interpretation as detailed [in the Petition.]” Pet. 10. Patent Owner asserts that “[t]he Petition does not raise a dispute as to any claim construction issues” and “Patent Owner does not believe the Board need resolve any claim construction issues at this stage.” Prelim. Resp. 6 (citing Pet. 9–10).

Construction is needed only for those terms “that are in controversy, and only to the extent necessary to resolve the controversy.” *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). There are no claim terms in controversy at this stage of the proceeding. Consequently, we need not construe any terms for our analysis.

B. Principles of Law Regarding Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence

of non-obviousness.⁶ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). A patent claim “is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR*, 550 U.S. at 418.

An obviousness determination based on a combination of references requires finding “both ‘that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016); *see KSR*, 550 U.S. at 418. Furthermore, an assertion of obviousness “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.” *KSR*, 550 U.S. at 418; *In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (a finding of a motivation to combine “must be supported by a ‘reasoned explanation’”).

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3)); *see also Intelligent Bio-Sys.*, 821 F.3d at 1369. This burden of persuasion never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review). Therefore, to prevail in an *inter partes* review, Petitioner must explain how

⁶ At this stage of the proceeding, Patent Owner has not presented objective evidence of non-obviousness.

the proposed combination of prior art would have rendered the challenged claims unpatentable. At this preliminary stage, we determine whether the information presented in the Petition shows there is a reasonable likelihood that Petitioner would prevail in establishing that at least one of the challenged claims would have been obvious over the proposed combinations of prior art.

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quoting *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962, (Fed. Cir. 1986)). Furthermore, the prior art itself can reflect the appropriate level of ordinary skill in the art. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Here, Petitioner asserts a person of ordinary skill in the art at the time of the invention of the '313 patent would have “had a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and 2–3 years of practical engineering experience relating to information security systems that employ cryptographic keys to encrypt/decrypt digital data.” Pet. 9 (citing Ex. 1003 ¶¶ 1–20, 37–41). Mr. Wechselberger supports Petitioner’s position and further testifies that “[a]dditional education could substitute for professional experience, or

significant experience in the field could substitute for formal education.”
Ex. 1003 ¶ 40.

Patent Owner does not assert a different level of skill in the art at the time of the alleged invention and does not dispute Petitioner’s proposed level of skill. Prelim. Resp. 6.

For the purposes of this Decision, we adopt Petitioner’s level of ordinary skill in the art because it appears consistent with the problems addressed in the ’313 Patent and the prior art of record.

III. ANALYSIS

A. *Summary of References*

1. *Peterka (Ex. 1005)*

Peterka is a U.S. patent application publication titled “Intial [*sic*] Free Preview for Multimedia Multicast Content.” Ex. 1005, code (54). Peterka relates to “providing a preview portion of a program distributed to clients on the network.” *Id.* ¶ 2.

Peterka discloses a content distribution system for downloading a streaming media to one or more client computers. Ex. 1005 ¶ 38. Peterka also describes various purchase mechanisms that allow a client to purchase content. *See id.* ¶¶ 50–55. For example, Peterka describes “Pay-By-Time (PBT)” as “[a] purchase mechanism in which the client pays for the time duration of the content that was actually watched.” *Id.* ¶ 53. Peterka explains that content may be divided into “pay segments,” to which “segment keys” are assigned. *Id.* ¶ 80. In the PBT model implementation, the client starts receiving the content when it negotiates encryption keys with the caching server and the client will “monitor the expiration time for each pay period and request a new set of keys from the caching server.” *Id.* ¶ 82. According to Peterka, “[i]f the viewer stops watching or moves to another

service the client will not request new keys or it will actively notify the caching server that it wants to leave the current multicast session.” *Id.*

One embodiment of Peterka is shown in Figure 7A, reproduced below.

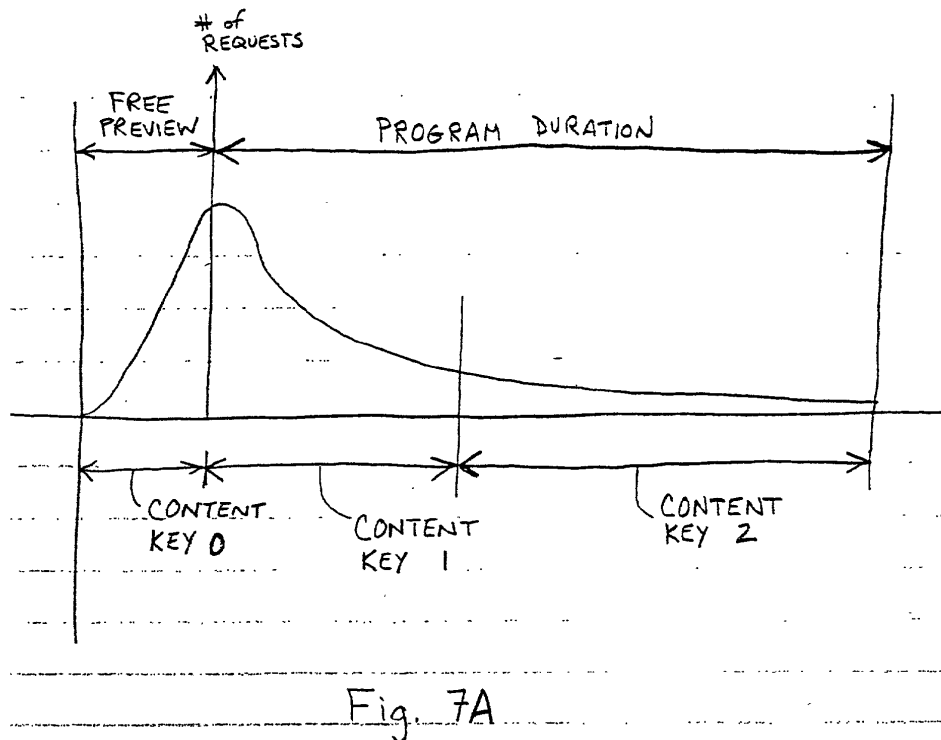


Figure 7A of Peterka, above, is “a plot showing the number of requests for a program versus the program duration.” Ex. 1005 ¶ 91; *see also id.* ¶ 21 (“showing exemplary distribution of cryptographic keys during portions of a program”). Peterka explains that “an initial free preview period provides for client computers to request an initial key for viewing an encrypted portion of the program.” *Id.* ¶ 91. Peterka also explains that the distribution of content keys 0, 1, and 2 is shown at the bottom of Figure 7A. *Id.* ¶ 92. According to Peterka, content key 0 is provided to the user for obtaining the free preview, while content keys 1 and 2 are required to decrypt the remainder of the program content. *Id.* For example, content key 1 may be a group key and

content key 2 may be the actual content encryption key delivered only to those clients that purchased the content. *Id.* ¶ 93. In this way, clients first view a free preview, and those who make a decision to buy use the group key to allow their viewing experience to continue. *Id.* Peterka explains that “[t]he server would deliver the Key 2 during this time, so that those viewers could continue viewing the remainder of the content in a continuous fashion.” *Id.*

Peterka describes various models for distributing keys to clients. Ex. 1005 ¶ 105. For example, Peterka describes a “Pull” model, under which “each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.” *Id.*; *see also id.* ¶ 106, Fig. 8 (describing the pull key distribution model).

Peterka also describes a signaling method to indicate the implementation of a new key. Ex. 1005 ¶ 117. For example, when using a “Real-Time Transport Protocol” (RTP) packet for distributing content, a field is inserted between the header portion and the payload portion of the packet to indicate a key change. *Id.*; *see also id.* ¶ 43. The inserted field may be “an extended header” indicating that “the content key for the payload portion of the packet has changed,” or “it could indicate that the next occurring payload portion could be decrypted utilizing the new content key or such similar implementation.” *Id.* ¶ 117.

2. *Suzuki (Ex. 1006)*

Suzuki is a Japanese patent application publication titled “Key Exchange Method in Multicast Distribution System.” Ex. 1006, code (54). Suzuki’s object is to “provide a key exchange method in a multicast distribution system that prevents eavesdropping by encrypting data with a

different key at regular intervals during multicast distribution, thereby eliminating the confirmation delay (key switch delay) that occurs when changing (exchanging) a key and enabling real-time data processing.” *Id.* ¶ 11.

Suzuki describes a multicast distribution system with a content server and a key management server, wherein (1) the content server “issues a key creation request to the key management server to request the creation of the next key to be used when the remaining validity time of the key in use reaches the first setting value (a value smaller than the initial value of the remaining validity time of the key in use and larger than 0)”; (2) a client “transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value (a value smaller than the first setting value and larger than 0)”; and (3) the key management server “creates the encryption key/decryption key to be used next in response to the key creation request received from the content server, . . . returns a key information response message regarding the encryption key to be used next (a message having key information that is a set of the encryption key to be used next, its key number, and its remaining validity time) to the content server, [and] returns a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time to the client when receiving a key information request from the client when the remaining validity time of the key in use reaches the second setting value.” Ex. 1006 ¶ 16; *see id.* at Figs. 3–4.

3. *Bocharov (Ex. 1007)*

Bocharov is a U.S. patent application publication titled “Delivering Cacheable Streaming Media Presentations.” Ex. 1007, code (54). Bocharov relates to a “smooth streaming system” that “provides a stateless protocol

between the client and server in which the server embeds incremental information in media fragments (i.e., chunks) that eliminates the usage of a typical control channel.” *Id.* ¶ 14.

According to Bocharov, “[t]he smooth streaming system receives media data in fragments from one or more encoders, creates an index of each fragment, and stores the fragments,” wherein “[e]ach fragment contains metadata and media content.” Ex. 1007 ¶¶ 14, 16. Bocharov explains that the smooth streaming system can provide clients with manifest information about available media fragments. *Id.* ¶ 21. For example, the system may receive a request for a client manifest from the client and create a manifest that the client can use “either to begin requesting ongoing live fragments, or to skip backwards in time to earlier portions of a presentation.” *Id.* ¶ 23. According to Bocharov, “[b]y combining the initially received manifest with subsequent manifests provided with each media fragment, the client can build an up to date manifest that includes complete information about the media event from the start up until the current time,” such that “[w]hen the media event completes, the client has a complete storyboard of the media event that the client can use for on-demand viewing of the media event.” *Id.* ¶ 24.

One embodiment of Bocharov is shown in Figure 5, reproduced below.

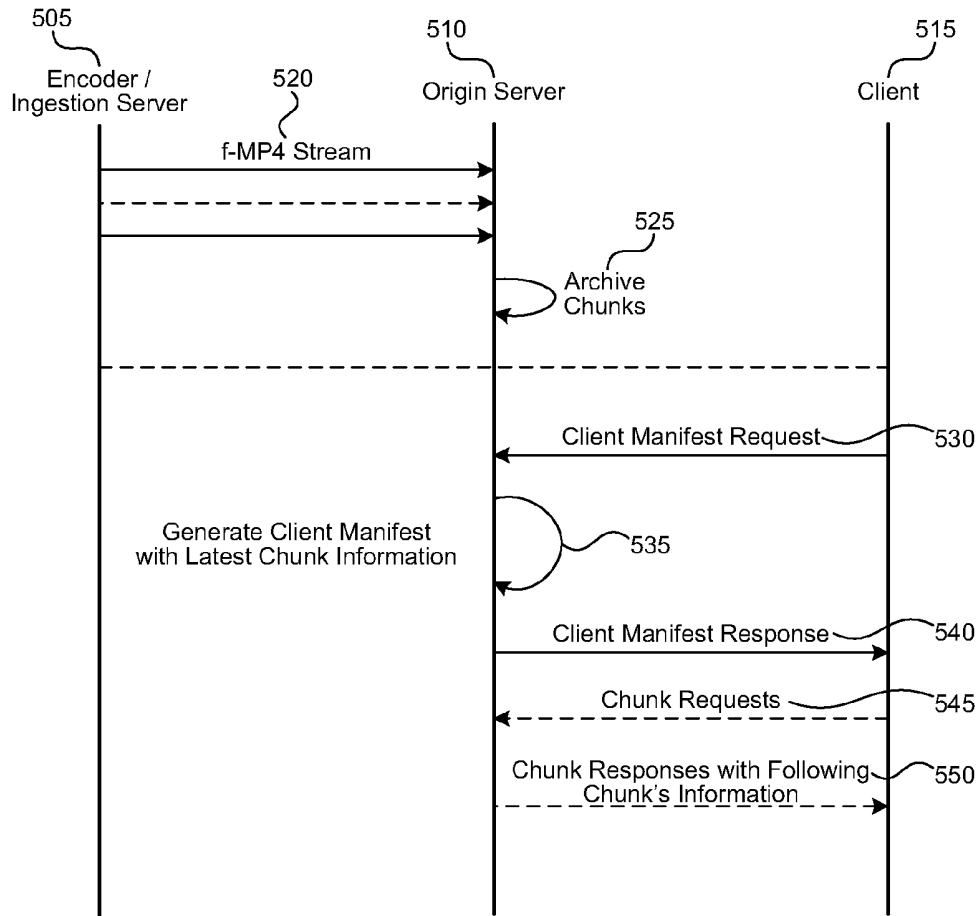


FIG. 5

Figure 5 of Bocharov, above, shows “a data flow diagram that illustrates the flow of media fragments from an encoder to an origin server to a client.”

Ex. 1007 ¶ 53. Figure 5 shows the encoder 505 continuously providing the origin server 510 with media data 520, which may include fragments of, for example, an MP4 stream. *Id.* According to Bocharov, upon receiving a manifest request 530 from a client 515, the origin server 510 generates a client manifest 535 based on the latest media fragment information and provides a client manifest response 540 to the client 515. Bocharov further describes that “[t]he client 515 then sends one or more media fragment requests 545, and the origin server 510 responds 550 with the requested

media fragment and potentially information about subsequent media fragments.” *Id.*

4. *Peterka308 (Ex. 1008)*

Peterka308 is a U.S. patent application publication titled “Method and Apparatus for Providing a Secure Trick Play.” Ex. 1008, code (54).

Peterka308 relates to “the management of rights associated with audio/visual content.” *Id.* ¶ 3. Peterka308 describes a process that “composes a content license for a set of content that has a corresponding expiration content rule indicating a time limit on temporary playability of the set of content.” *Id.*

¶ 9. The set of content is characterized as a plurality of segments, wherein each segment has a segment length according to a predetermined time interval. *Id.* According to Peterka308, “the process generates a unique content encryption key for each of the segments so that each of the segments is encrypted to form a plurality of encrypted segments.” *Id.* Peterka308 further describes that “the process inserts a plurality of time stamps into the content license,” wherein “[e]ach of the time stamps corresponds to one of the encrypted segments and indicates a relative time from a recording start time to start of the encrypted segment.” *Id.*

According to Peterka308, a content encryption key (“CEK”) is generated for each segment “that is utilized to re-encrypt the content for storage on the hard drive . . . or other media storage, and to decrypt the re-encrypted content during playback.” Ex. 1008 ¶ 22. Peterka308 also describes “[a]n expiration content rule, e.g., copy never content rule,” which “establishes a predetermined amount of time for which the content may be temporarily stored [in, e.g., a hard drive] to allow for the trick play features, e.g., ninety minutes.” *Id.* ¶ 23.

Peterka308 describes one embodiment where “a time stamp, which indicates the relative time value from the beginning of the recording to the start of the segment, is generated and stored at the time that each unique CEK is determined” and “[e]ach time stamp is dynamically added to the content license as the recording progresses.” Ex. 1008 ¶ 25. According to Peterka308, “[d]uring playback, the master key and the time stamp for a particular segment may be utilized, at least in part, to derive the CEK for that segment so that the encrypted content for that segment stored in the hard drive . . . or other media storage may be decrypted.” *Id.*

5. *Chen (Ex. 1009)*

Chen is a European patent application publication titled “Method and System for Encrypting Material for Distribution.” Ex. 1009, code (54). Chen relates to “conditional access and copy protection techniques . . . for interactive, on-demand digital program content such as video-on-demand (VOD) programming distributed via cable and satellite networks.” *Id.* ¶ 1. Chen discloses techniques to “pre-encrypt VOD material with a changing cryptographic key and to convey this information to VOD servers so that the VOD servers can send out the corresponding ECMs (Entitlement Control Messages) when the encrypted content is delivered to a consumer’s digital set top.” *Id.* ¶ 8. According to Chen, “streaming content is encrypted by segmenting the content into a plurality of crypto periods, and encrypting the content for each of a plurality of crypto periods with a different cryptographic key.” *Id.* ¶ 10; *see also id.* ¶ 34 (describing “four different basic schemes (techniques, methodologies) for breaking up (subdividing, segmenting, sectioning) the content to be encoded/encrypted into a plurality of ‘crypto periods’, covered by different cryptographic keys”—“Fixed

crypto period,” “Fixed number of packets,” “Fixed ‘marker’ count,” and “Random crypto period”).

B. Claims 1–4, 6, 7, 11–14, 16, and 17 Allegedly Rendered Obvious by Peterka Alone or in Combination with Suzuki

Petitioner contends that Peterka alone or in combination with Suzuki teaches or suggest every limitation of claims 1–4, 6, 7, 11–14, 16, and 17. Pet. 17–51. Patent Owner disagrees. Prelim. Resp. 1–2, 7–20. Patent Owner specifically challenges whether Petitioner has shown that Peterka alone or with Suzuki teaches limitation ([1B]) “the live media playback request response comprising content encryption keys and content encryption key identifiers,” as required by challenged independent claims 1 and 11. *Id.* at 7–16 (emphasis omitted). Patent Owner further challenges whether Petitioner has demonstrated a reason to combine Peterka with Suzuki. *Id.* at 16–20.

1. Analysis of Independent Claim 1

a) Limitation [1PRE]

Claim 1 is directed to:

[1PRE] A method for handling secure distribution of live video content comprising:

Ex. 1001, 12:23–24.

Petitioner contends that Peterka discloses the preamble, pointing to Peterka’s disclosure of a “[m]ethod of providing program material to multiple clients,” “encrypted material . . . provided for distribution to a client, e.g., by a content exchange such as a metropolitan video exchange or an origin server,” “[e]ncryption keys . . . distributed to clients to facilitate reception of the program content,” and “live content.” Pet. 18 (citing Ex. 1005 ¶¶ 12, 58, 83, 94, Figs. 1, 3; Ex. 1003 ¶ 73) (emphasis omitted).

Patent Owner does not dispute Petitioner’s contentions for the preamble. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Generally, when analyzing a claim preamble, we must determine whether to treat the preamble term as a claim limitation. *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010). In the present case, we need not reach a determination on whether the preamble is limiting because we find the prior art teaches the preamble. Specifically, Peterka’s disclosure in block 304 of encrypted material being provided for distribution to a client,” e.g. “by a content exchange such as a metropolitan video exchange or an origin server” appears to meet the scope of the preamble. *See* Ex. 1005 ¶ 83; *see also* Pet. 18 (citing Ex. 1005 ¶ 94) (“[E]ncryption keys can be distributed to clients to facilitate reception of the program content.”).

Accordingly, we find Petitioner’s contentions for the preamble persuasive, and, therefore, we need not determine whether the preamble is limiting for purposes of this Decision.

b) Limitation [1A]

Claim 1 recites the steps:

[1A] sending a request for live media playback; receiving a live media playback request response,

Ex. 1001, 12:25–26.

Petitioner contends that Peterka discloses “clients request[ing] access to media content—e.g., under Peterka’s pay-by-time distribution scheme—and then receiv[ing] encryption keys to gain access to at least a portion of a media stream,” and “Peterka’s disclosed client-initiated requests to access media, e.g., program content, are each sending a request for live media

playback as recited in claim 1.” Pet. 18–19 (citing Ex. 1005 ¶¶ 80–82, 91–92, 141–143, Figs. 7A–7B, 20A–20B; Ex. 1003 ¶¶ 74–75) (emphasis omitted); *see id.* at 50.

Petitioner provides the following colorized version of Peterka’s Figure 7B to illustrate its contentions:

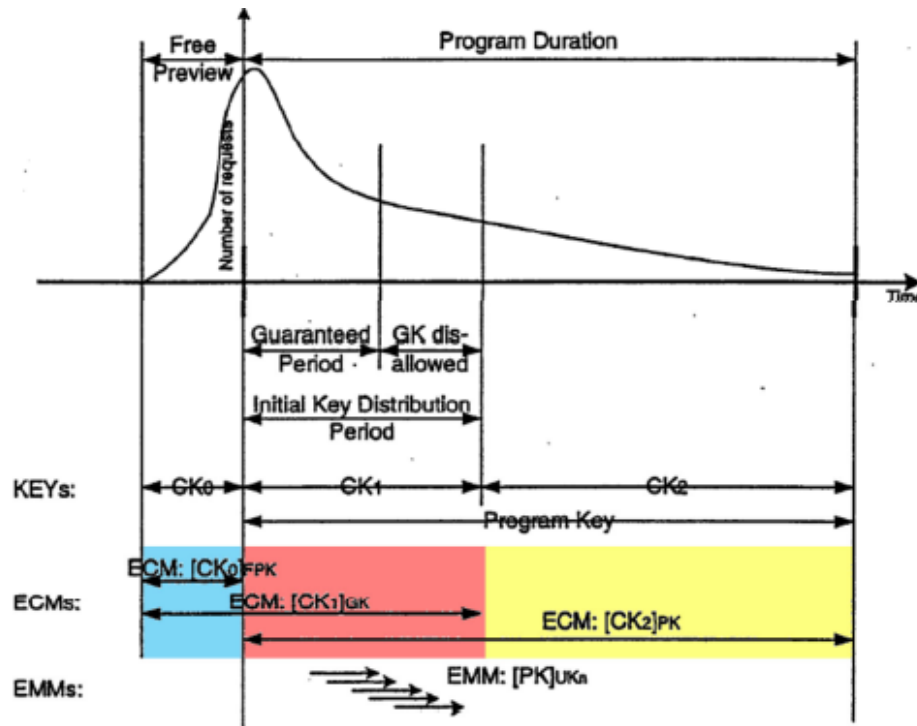


Fig. 7B

Pet. 20. Peterka’s Figure 7B above with Petitioner’s coloring shows content keys CK_0 , CK_1 , and CK_2 distributed in separate entitlement control messages (ECMs), wherein CK_0 and CK_1 are distributed for each request received during a free preview period (blue); ECMs with CK_1 are distributed to clients before the period in which CK_1 is used (red); and ECMs with CK_2 are distributed to clients before the period in which CK_2 is used (yellow). *Id.* at 20–21 (citing Ex. 1005 ¶ 130; Ex. 1003 ¶ 78). Petitioner asserts that

Peterka’s “multiple EMMs/ECMs sent to clients in response to a particular request for live media playback collectively constitute a live media playback request response received by a client, as claimed.” *Id.* at 21 (citing Ex. 1005 ¶¶ 104–106, 121, 122–125, Figs. 7B, 8; Ex. 1003 ¶¶ 79–80) (emphasis omitted); *see id.* at 50.

Patent Owner does not dispute Petitioner’s contentions for this limitation. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed Peterka, on this record, we agree with Petitioner that Peterka discloses sending a request for live media playback and receiving a live media playback request response, as recited in claim 1. *See* Pet. 18–22, 50. Specifically, we are persuaded that Peterka’s “pay-by-time” embodiment sufficiently discloses that after a viewer’s selection/request, the client system negotiates encryption keys with the caching sever in order to start receiving video content. Peterka explains that encryption keys are distributed in response to requests for live media playback and we are satisfied that indicates a live media playback request response is received by a client server as required by claim 1. *See* Ex. 1005 ¶¶ 104–106, 121, 122–125, Figs. 7B, 8.

c) Limitation [1B]

Claim 1 recites:

[1B] the live media playback request response comprising content encryption keys and content encryption key identifiers;

Ex. 1001, 12:26–28.

Petitioner contends that Peterka’s ECMs/EMMs contain information responsive to a request to access/play at least a portion of a stream. Pet. 22 (citing Ex. 1005 ¶¶ 104–106, 121–125, Fig. 7B; Ex. 1003 ¶¶ 81–82).

(1) *Content Encryption Keys*

Petitioner contends that “Peterka’s ECMs/EMMs carry keys to clients, including ‘content key[s]’ (‘CKs’) that were ‘used to encrypt the content itself’ and are used by the client to decrypt content (content encryption keys).” Pet. 23 (citing Ex. 1005 ¶¶ 101, 106, 116, 121) (emphasis omitted); *see id.* at 49.

Patent Owner does not dispute Petitioner’s contention regarding Peterka’s teaching of content encryption keys. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

(2) *Content Encryption Key Identifiers*

(a) *Peterka*

Petitioner next contends that “Peterka discloses that each ECM/EMM includes ‘a sequence number or a time stamp to protect against replay attacks.’” Pet. 24 (quoting Ex. 1005 ¶ 121) (emphasis omitted). According to Petitioner, “[b]ecause the sequence number/timestamp is unique to each ECM/EMM (to prevent replay attacks), and each ECM/EMM carries a different content encryption key . . . , the sequence number/timestamp each constitutes a unique content encryption key identifier.” *Id.* (citing Ex. 1003 ¶ 89) (emphasis omitted).

In the alternative, Petitioner argues that, “in view of, e.g., [Peterka’s] Fig. 7B, which shows delivery of content keys with unique designations—CK₀, CK₁, CK₂,” a person of ordinary skill would have been motivated “to implement Peterka’s client to receive and use a key identifier to identify the

content key in an ECM/EMM.” Pet. 25 (citing Ex. 1003 ¶ 92) (emphasis omitted). According to Petitioner, “[i]n systems like Peterka’s, where multiple keys are utilized, [persons of ordinary skill] would have recognized the need to differentiate between keys, would have been motivated to do so with key identifiers, and would have reasonably expected success.” *Id.* (citing Ex. 1005 ¶¶ 80, 122, 130, Fig. 7B; Ex. 1003 ¶¶ 91–94).

Patent Owner disagrees with Petitioner’s arguments and contends Peterka’s teaching does not meet the limitation of “content encryption key identifiers.” Prelim. Resp. 7–14. According to Patent Owner, Petitioner “acknowledges that the ‘sequence number/timestamp’ that Petitioner relies upon ‘is unique to each ECM/EMM,’” admitting that “the ‘unique identifier’ it relies upon from Peterka is assigned to the message carrying a content encryption key, and not to the key itself.” *Id.* at 8 (citing Pet. 24) (emphasis omitted). As such, Patent Owner argues that Petitioner’s “reliance on Peterka’s message identifier thus cannot meet its burden of unpatentability as to limitation 1B.” *Id.* at 9 (emphasis omitted).

Patent Owner also disagrees with Petitioner’s alternative argument that a person of ordinary skill would have been motivated to implement Peterka’s client to receive and use a key identifier. Prelim. Resp. 9 (citing Pet. 25). Patent Owner contends that “[s]ince Peterka already assigns a unique identifier to the message carrying each individual key, there would be no need, motivation, or benefit from further assigning a unique identifier to the key contained in each such message.” *Id.* at 10 (emphasis omitted). According to Patent Owner, “the Federal Circuit has repeatedly held that a [person of ordinary skill] would not have a motivation to modify a reference to solve a problem that the reference itself did not have, even if other art may have taught the benefits of the modification under other circumstances.”

Id. (citing *In re NuVasive*, 842 F.3d at 1383–84; *Duke Univ. v. BioMarin Pharm. Inc.*, 685 F. App’x 967, 978–79 (Fed. Cir. 2017); *In re Schweickert*, 676 F. App’x 988, 993–96 (Fed. Cir. 2017); *In re Anova Hearing Labs, Inc.*, 809 F. App’x. 840, 843 (Fed. Cir. 2020)) (emphasis omitted).

In response to Petitioner’s contention that “Peterka itself shows delivery of content keys with unique designations—CK₀, CK₁, and CK₂,” Patent Owner asserts that “Peterka simply uses CK₀, CK₁, and CK₂ to distinguish between the keys shown in its Figure 7B for purposes of clarity in Peterka’s specification” and “never teaches sending CK₀, CK₁, and CK₂, or any key identifier, to a client as part of a media playback request response, nor does the Petition identify any evidence of Peterka doing so.” Prelim. Resp. 14 (citing Ex. 1005 ¶ 122) (emphasis omitted).

At this stage of the proceeding, we are persuaded Petitioner has the better argument. Specifically, we are persuaded Patent Owner reads the term “content encryption key identifiers” too narrowly to mean an identifier that is tied directly to a content encryption key. The ’313 patent discloses that workflow manager (WFM) 102 “generates an initial content encryption key” and simply “assigns it a content encryption key identifier.” *See* Ex. 1001, 6:1–2. According to the ’313 patent the content encryption key identifier can be created in several different ways: (1) the identifier can initially be set to zero and all future content encryption key identifiers are based on a relative offset to the initial content encryption key identifier; (2) it can be based off segment numbers; or (3) it can be based off the wall clock time offset. *Id.* at 6:2–14. This appears to correspond closely to Peterka’s disclosure of content keys identified as C₀, C₁, and C₂, without the requirement that the identifier actually being tied directly to the key itself. *See* Ex. 1005 ¶ 122, Figs 7a, 7b.

Additionally, Patent Owner’s argument that “Peterka simply uses CK₀, CK₁, and CK₂ to distinguish between the keys shown in its Figure 7B for purposes of clarity in Peterka’s specification” and “never teaches sending CK₀, CK₁, and CK₂, or any key identifier, to a client as part of a media playback request response,” appears at odds with Peterka’s disclosure of a first entitlement control message for a free preview period in which a content key CK₀ is encoded with a free preview key (ECM: [CK₀] FPK), and then a second entitlement control message conveying a second content key encrypted with the program key (ECM: [CK₂]PK). Ex. 1005 ¶ 122.

According to Peterka, an entitlement control messages (ECM) with only one content encryption key is sent from a sever to a client computer and that ECM includes a unique sequence number (CK₀, CK₁, CK₂, etc.) in its headers that appears to correspond to both the content and the encryption key within the ECM. *Id.* ¶ 121. Therefore, we are persuaded at this stage of the proceeding that Peterka appears to assign an identifier to each content encryption key in a similar manner as at least one of the methods taught in the ’313 patent. *See* Ex. 1001 6:1–6. Nonetheless, we do not assess Petitioner’s position that Peterka alone render the challenged claim obvious. Rather, as discussed below, we address Petitioner’s contentions regarding the combined teachings of Peterka with Suzuki.

(b) Peterka-Suzuki

Petitioner also contends that the combined teaching of Peterka with Suzuki meets this claim limitation. Pet. 49. Specifically, Petitioner argues that Suzuki’s teachings regarding “key numbers” and “remaining validity times” corresponds to each received “content encryption key” of Peterka. According to Petitioner, these Suzuki’s “key numbers” act to keep track of keys and to uniquely identify keys; thus, they qualify as content encryption

key identifiers, as claimed. *Id.* at 46 (citing Ex. 1006 ¶¶ 71–84; Ex. 1003 ¶ 150), 49 (citing Ex. 1003 ¶ 159). Petitioner further argues that Suzuki teaches “key information” obtained by “submitting a ‘key information request’ to a server, which responds with a ‘key response message’ that includes (1) the current and next keys (‘key A,’ ‘key B’), (2) each key’s ‘key number’ (‘key number A,’ ‘key number B’), and (3) each key’s ‘remaining validity time.’” *Id.* at 46–47 (citing Ex. 1006 ¶¶ 72–77, Figs. 5–6; Ex. 1003 ¶ 151). Petitioner asserts that Suzuki’s “[k]ey number” is used to ‘identify[] the key,’ allowing a client to associate keys with their respective ‘remaining validity time[s]’ (e.g., in a table) and to help the client keep track of keys, for example when determining which key to apply when decrypting a segment of content.” *Id.* at 48 (citing Ex. 1006 ¶¶ 30, 43–48, 80, Fig. 2; Ex. 1003 ¶ 153) (second and third alterations in original).

Petitioner contends that a person of ordinary skill “would have had reasons to implement Peterka’s client in view of Suzuki to acquire and use ‘key information’ about a next key—its ‘remaining validity time’ and ‘key number’—at a set time before the expiration of the current key, and thereby facilitate timely key acquisition and use.” Pet. 48 (citing Ex. 1006 ¶¶ 76–77, 80–81, 43–48; Ex. 1003 ¶ 155) (emphasis omitted). According to Petitioner, “[t]his would have allowed a [person of ordinary skill] to ‘eliminat[e] the confirmation delay’ during key changes, and realize Peterka’s embodiment where ‘each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.’” *Id.* (citing Ex. 1006 ¶ 11; Ex. 1005 ¶ 105) (third alteration in original).

Patent Owner disagrees with Petitioner’s arguments and contends the combination of Peterka and Suzuki fails to meet the limitation of “content

encryption key identifiers.” Prelim. Resp. 14–20. First, Patent Owner asserts that “Suzuki merely teaches the use of a ‘key number A,’ representing the current key in use, and a ‘key number B,’ representing the next key to be used.” *Id.* at 15 (citing Ex. 1006 ¶¶ 72–77; Pet. 46). Patent Owner further asserts that “any key could be named ‘key number A’ or ‘key number B’ simply based on whether that key is the current key or the next key—a nomenclature that is not ‘unique’ to any particular key,” even though “the ’313 Patent teaches and claims unique key identifiers.” *Id.* (citing Ex. 1001, 3:38–40) (emphasis omitted). Patent Owner further asserts that since “Suzuki only teaches identifying keys as the current key or the next key, and does not teach providing unique values to keys,” “Suzuki cannot support the Petition’s purported motivation of ‘providing unique values (such as key numbers) to keys.’” *Id.* at 16 (quoting Pet. 48).

Patent Owner next contends that even though Petitioner “cites to Suzuki for the alleged benefit of ‘eliminating confirmation delay during key changes,’” “the Petition does not show that Peterka had any problem of ‘confirmation delay during key changes,’ or that modifying Peterka to add key identifiers would have solved any such non-existent problem.” Prelim. Resp. 16 (quoting Pet. 48) (emphasis omitted). Patent Owner asserts that Petitioner’s “‘confirmation delay’ motivation . . . further fails even based on Suzuki’s own teachings because Suzuki does not teach that using key identifiers improves confirmation delay.” *Id.* at 17.

Next, Patent Owner asserts that “the Petition’s motivation of ‘facilitate[ing] timely key acquisition and use’ likewise fails because the Petition does not show how adding key identifiers to Peterka would have actually ‘facilitated timely key acquisition and use.’” Prelim. Resp. 17 (citing *In re NuVasive*, 842 F.3d at 1384) (alteration in original)).

Finally, Patent Owner contends that since “Peterka does not leave a gap as to how clients should determine when to apply a new key, or how clients should identify key expiration times,” “Peterka . . . has no need for unique key identifiers to realize Peterka’s embodiment where each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.” Prelim. Resp. 19–20 (citing Pet. 48) (internal quotation marks omitted).

As explained previously, we are persuaded at this time by Petitioner’s position over Peterka. Specifically, Peterka’s teachings appear to be sufficient to render obvious the recited “content encryption key identifier” for at least two reasons. First, Peterka’s sequence number/time stamp assigned to each ECM/EMM (Ex. 1005 ¶ 121) appears to be similar to the ’313 patent’s example of content encryption identifiers based off of segment number or wall clock time offset from the time the initial content encryption key identifier was generated (Ex. 1001, 6:9–14). Second, Peterka’s designation of content keys as CK₀, CK₁, CK₂ (Ex. 1005 ¶ 122, Figs. 7A–7B) appears to be similar to the ’313 patent’s example of content encryption identifiers based off a next sequential integer value, offset from the previous content encryption key identifier (Ex. 1001, 6:6–9). Additionally, we understand that Patent Owner agrees that Peterka “uses CK₀, CK₁, and CK₂ to *distinguish between the keys* shown in its Figure 7B for purposes of clarity in Peterka’s specification.” See Prelim. Resp. 14 (emphasis added).

We also are persuaded based on the current record that Suzuki’s teachings bolster Peterka’s teaching of this limitation. See Ex. 1006 ¶¶ 33, 36, 43–48, 59, 72–77, 80–81, Figs. 4–6. Moreover, we are persuaded that a person of ordinary skill in the art at the critical time would have had reason

to apply the teachings of Suzuki to Peterka. Specifically, we credit the testimony of Mr. Wechselberger, who testifies that (1) Peterka and Suzuki are in the same field of art and (2) both references disclose “periodically” changing keys that protect distributed content. Ex. 1003 ¶ 154 (citing Ex. 1006 ¶¶ 3, 12; Ex. 1005 ¶¶ 82, 110). Mr. Wechselberger explains that an ordinarily skilled artisan would have recognized the importance of identifiers “to differentiate amongst keys, and that providing unique values (such as key numbers) to keys would ensure that the system does not confuse keys.” *Id.* ¶ 153. According to Mr. Wechselberger, an ordinarily skilled artisan “would have had reasons to implement Peterka’s client in view of Suzuki to acquire and use ‘key information’ about a next key—its ‘remaining validity time’ and ‘key number’—at a set time *before* the expiration of the current key, and thereby facilitate timely key acquisition and use.” *Id.* ¶ 155 (citing Ex. 1006 ¶¶ 76–77, 80–81, 43–48) (emphasis added). At this stage of the proceeding, and crediting the testimony of Mr. Wechselberger, we are persuaded that the combined teachings of Peterka and Suzuki would have allowed a person of ordinary skill in the art “to ‘eliminat[e] the confirmation delay’ during key changes, and realize Peterka’s embodiment where “each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.” *See* Ex. 1006 ¶ 11; Ex. 1005 ¶ 105.

Thus, after review of the arguments and evidence, we find that Petitioner has provided adequate explanation and supporting evidence that Peterka alone or in combination with Suzuki teaches live media playback request response comprising content encryption keys and content encryption key identifiers, as recited in claim 1. We also are persuaded by Petitioner’s

position that a person of ordinary skill in the art at the critical time would have a reason to combine the teachings of Peterka with that of Suzuki.

d) Limitation [1C1]

Claim 1 recites the step:

[1C1] receiving encrypted live media content and manifest files from a content delivery server,

Ex. 1001, 12:29–30.

Petitioner contends that “Peterka discloses a device (e.g. client computer 112) receiving encrypted live media content from a content delivery server (e.g., origin 108, a content exchange 116, or caching server).” Pet. 26 (citing Ex. 1005 ¶¶ 38, 39–40, 60, 71, 83, 135, Figs. 1, 19; Ex. 1003 ¶ 97) (emphasis omitted); *see id.* at 50. Petitioner argues that “Peterka expressly discloses a client playing a ‘streaming media’ content object ‘during download’” because content is encrypted before distribution and then streamed as “live content” to multiple consumers at once. *Id.* at 27 (citing Ex. 1005 ¶¶ 6, 38, 58); Ex. 1003 ¶ 98).

Petitioner also contends that Peterka “renders obvious ‘receiving . . . manifest files from a content delivery server,’ as claimed.” Pet. 30 (emphasis omitted). According to Petitioner, while “Peterka does not explicitly describe ‘manifest files,’” “manifest files were well-known as ‘conventional’ features of media ‘streaming platforms’ like those taught by Peterka which stream, e.g., segments of MPEG-4 format media at various bit rates.” *Id.* at 27 (citing Ex. 1005 ¶¶ 53–54, 119; Ex. 1003 ¶¶ 99–100). Petitioner argues that Peterka describes a client adjusting a bit rate based on the user selection and that “it would have been obvious to implement Peterka’s client to retrieve from the content delivery server both the content itself and manifest files describing the content, which at minimum included

information regarding available ‘quality (i.e., bit rates)’ that would allow the disclosed bit-rate adjustments.” *Id.* at 28–29 (citing Ex. 1005 ¶¶ 54, 59, 119; Ex. 1003 ¶ 105). Petitioner then asserts that “[i]t also would have been obvious to implement Peterka’s client, which retrieves media streams divided into segments, to retrieve multiple manifest files from the content server, with each subsequent manifest file describing subsequent corresponding media segments.” *Id.* at 29 (citing Ex. 1005 ¶¶ 80–82, 91–93, 99–101, 122–125, Figs. 7A–7B; Ex. 1003 ¶ 106) (emphasis omitted).

Patent Owner does not dispute Petitioner’s contentions for this limitation. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed Peterka, on this record, we agree with Petitioner that Peterka discloses the recited claim limitation. Peterka specifically discloses that an “object can be played during download if it is a streaming media or can be stored for later display” where the content object “could be various types of information, such as audio, video, or data that is available to be downloaded from the network” and that “it can be used for multicasting and/or unicasting.” *See* Ex. 1005 ¶ 38. Peterka also discloses that the “multicasting program material is provided by providing encrypted program material for distribution to a client; providing a key for use by the client.” *Id.* ¶ 6. Accordingly, on this record, we agree with Petitioner that Peterka discloses or renders obvious receiving encrypted live media content and manifest files from a content delivery server, as recited in claim 1.

e) Limitation [1C2]

Claim 1 recites:

[1C2] wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content;

Ex. 1001, 12:30–35.

Petitioner asserts that Peterka teaches dividing encrypted live media content “into segments that are each encrypted with a different key.”

Pet. 30–31 (citing Ex. 1005 ¶¶ 80–82, 91–93, 99–101, 122–125, Figs. 7A–7B; Ex. 1003 ¶ 108). According to Petitioner,

A person of ordinary skill “understood that such segmented, encrypted live media content comprises one or more content encryption key rotation boundaries because Peterka teaches using different keys to encrypt different content segments, and key rotation boundaries occur each time a new key is needed to decrypt content (e.g., when a current key taught in Peterka expires).

Id. at 31 (citing Ex. 1003 ¶ 109; Ex. 1005 ¶¶ 105–106, 114–115, 116–117).

Petitioner further contends that a person of ordinary skill “understood that each content encryption key rotation boundary in Peterka’s segmented, encrypted media content is associated with a change to a different content encryption key to decrypt the received encrypted live media content, as claimed, because Peterka’s client applies different keys to decrypt the respective program content segments that occur before and after a given key rotation boundary (e.g., before and after a current key in Peterka expires, as discussed above).” *Id.* (citing Ex. 1003 ¶ 110).

Patent Owner does not dispute Petitioner's contentions for this limitation. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed Peterka, on this record, we agree with Petitioner that Peterka discloses the recited claim limitation. Peterka specifically discloses multicasting encrypted content that is decrypted using an encryption key that is provided to a client. *See* Ex 1005 ¶ 6. According to Peterka, the content can be audio, video, or data that can be multicast or unicast. *Id.* ¶ 38. We are persuaded that Peterka teaches dividing encrypted live media content “into segments that are each encrypted with a different key.” *Id.* ¶¶ 80–82, 91–93, 99–101, 122–125, Figs. 7A–7B; Ex. 1003 ¶ 108. Additionally, we are persuaded by Petitioner that a person of ordinary skill would have “understood that such segmented, encrypted live media content comprises one or more content encryption key rotation boundaries because Peterka teaches using different keys to encrypt different content segments, and key rotation boundaries occur each time a new key is needed to decrypt content (e.g., when a current key taught in Peterka expires).” *See* Pet. 31; Ex. 1005 ¶¶ 105–106, 114–115, 116–117.

Accordingly, on this record, we agree with Petitioner that Peterka discloses or renders obvious encrypted live media content comprising one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content, as recited in claim 1.

f) Limitation [1D]

Claim 1 recites the step:

[1D] applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary;

Ex. 1001, 12:36–38.

Petitioner contends that “Peterka’s client applies the applicable key to decrypt a segment of media before playing it.” Pet. 32 (citing Ex. 1005 ¶¶ 11, 91–93, 127, Fig. 7A; Ex. 1003 ¶¶ 111–112).

Patent Owner does not dispute Petitioner’s contentions for this limitation. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed the entirety of the current record, we agree at this stage of the proceeding with Petitioner that Peterka discloses or renders obvious applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary, as recited in claim 1. *See* Ex. 1005 ¶¶ 6, 7, 11, 12, 83, 89–93, 122, 127, Fig. 7A.

g) Limitation [1E]

Claim 1 recites the step:

[1E] prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and

Ex. 1001, 12:39–42.

Petitioner asserts that “Peterka discloses a client device issuing a request ahead of the expiration of a current key (prior to reaching a first key rotation boundary) to retrieve a new key (obtain a second content encryption

key) that is . . . to be used after the first content encryption key rotation boundary is reached.” Pet. 32 (citing Ex. 1005 ¶¶ 105–106; Ex. 1003 ¶ 113) (emphasis omitted). Petitioner points to Peterka’s disclosure that “[u]nder the pull model, each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.” *Id.* (quoting Ex. 1005 ¶ 105) (emphasis omitted).

Patent Owner does not dispute Petitioner’s contentions for this limitation. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed the entirety of the current record, we agree at this stage of the proceeding with Petitioner that Peterka discloses or renders obvious obtaining, prior to reaching the first key rotation boundary, a second content encryption key, which is used after the first content encryption key rotation boundary is reached, as recited in claim 1. *See* Ex. 1005 ¶¶ 105–106

h) Limitation [1F]

Claim 1 recites the step:

[1F] applying the second content encryption key for content decryption after the key rotation boundary is reached.

Ex. 1001, 12:43–44.

Petitioner contends that “Peterka discloses applying the new key it requested (the second content encryption key for content decryption) after the key rotation boundary is reached—e.g., after the previous key expires.” Pet. 33 (citing Ex. 1005 ¶¶ 90, 92, 106, 108, 116; Ex. 1003 ¶ 115) (emphasis omitted). According to Petitioner, Peterka teaches that ““decryption by the

client’ occurs ‘by utilizing the cryptographic key that was requested’ prior to previous key’s expiration.” *Id.* (quoting Ex. 1005 ¶ 106).

Patent Owner does not dispute Petitioner’s contentions for this limitation. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed the entirety of the current record, we agree at this stage of the proceeding with Petitioner that Peterka discloses or renders obvious applying the second content encryption key for content decryption after the key rotation boundary is reached, as recited in claim 1. *See* Ex. 1005 ¶¶ 90, 92, 106, 108, 116.

2. *Analysis of Independent Claim 11 and Dependent Claims 2–4, 6, 7, 12–14, 16, and 17*

Petitioner provides arguments and evidence regarding independent claim 11, as well as dependent claims 2–4, 6, 7, 12–14, 16, and 17 in view of Peterka alone or in combination with Suzuki. Pet. 34–45, 49–51. Patent Owner relies on its arguments regarding claim 1 and has not provided separate arguments regarding Peterka alone or in combination with Suzuki in regards to these other challenged claims. *See* Prelim. Resp. 7 n.2. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition’s analysis of the other claimed subject matter not discussed in the previous sections and determine that the analysis is sufficient at this stage. Based on our review of the arguments and evidence submitted for independent claim 11, as well as dependent claims 2–4, 6, 7, 12–14, 16, and 17 and the reasons presented previously, we are persuaded for purposes of institution only that Petitioner has shown

sufficiently that Peterka alone or in combination with Suzuki teaches or suggests the limitations as recited in independent claim 11, as well as dependent claims 2–4, 6, 7, 12–14, 16, and 17.

3. *Summary regarding Challenges Based on Peterka alone or in combination with Suzuki*

Based on the current record, Petitioner has established a reasonable likelihood that it will prevail in demonstrating that claims 1–4, 6, 7, 11–14, 16, and 17 would have been obvious over Peterka alone or in combination with Suzuki.

C. *Claims 1–4, 6, 7, 9, 11–14, 16, 17, and 19 Allegedly Rendered Obvious by Peterka and Bocharov, or Peterka, Suzuki, and Bocharov*

Petitioner provides arguments and evidence regarding claims 1–4, 6, 7, 9, 11–14, 16, 17, and 19 in view of the combined teachings of Peterka and Bocharov, or the combined teachings of Peterka, Suzuki, and Bocharov. Pet. 51–63. Patent Owner relies on its previously discussed arguments regarding Peterka alone or with Suzuki in regards to the “content encryption key identifiers” limitation. *See* Prelim. Resp. 7 n.1. Patent Owner has not provided separate arguments regarding the combined teachings of Peterka and Bocharov, or the combined teachings of Peterka, Suzuki, and Bocharov in regards to these challenged claims. *See generally id.* Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition’s analysis and determine that the analysis is sufficient at this stage. Based on our review of the arguments and evidence submitted for claims 1–4, 6, 7, 9, 11–14, 16, 17, and 19, we are persuaded for purposes of institution only that Petitioner has shown sufficiently that Peterka in combination with Bocharov or in combination

with Suzuki and Bocharov teaches or suggests the limitations as recited in claims 1–4, 6, 7, 9, 11–14, 16, 17, and 19.

D. Claims 5 and 15 Allegedly Rendered Obvious by Peterka, Bocharov, Peterka308, and Chen

Claim 5 recites

The method of claim 1, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

Ex. 1001, 12:55–57.

Claim 15 recites

The computerized device of claim 11, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.

Ex. 1001, 14:15–17.

Petitioner provides arguments and evidence regarding dependent claims 5 and 15 in view of Peterka in combination with Bocharov, Peterka308, and Chen. Pet. 63–67. For example, according to Petitioner, “Peterka308 proposes using a ‘time stamp’ to derive the appropriate content encryption key for a ‘segment’ of encrypted media content, where the ‘time stamp’ indicates the ‘relative time value’ from the beginning of the media content to the start of the segment.” *Id.* at 64 (citing Ex. 1008 ¶ 25). Petitioner asserts that a person of ordinary skill in the art “would have sought to apply [in Peterka’s system] Peterka308’s suggested use of segment locators (e.g., timestamps) as content encryption key identifiers to provide a more robust method of signaling to client devices which content encryption key (e.g., which CK) to apply at the start of each segment, and would have reasonably expected success doing so.” *Id.* (citing Ex. 1003 ¶¶ 196–198).

Petitioner contends that “Peterka308 discloses content encryption key identifiers in the form of ‘time stamps,’ which a [person of ordinary skill] understood were predictable based on a predetermined known progression (e.g., every ‘five minutes has elapsed’).” *Id.* at 66 (citing Ex. 1008 ¶¶ 24, 29, 32) (emphasis omitted).

Patent Owner relies on its previously discussed arguments regarding Peterka alone or in combination with Suzuki in regards to the “content encryption key identifiers” limitation. *See* Prelim. Resp. 7 n.1. Patent Owner has not provided separate arguments regarding Peterka in combination with Bocharov, Peterka308, and Chen in regards to these challenged claims. *See generally id.* Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

We have reviewed the Petition’s analysis and determine that the analysis is sufficient at this stage. Based on our review of the arguments and evidence submitted for dependent claims 5 and 15, we are persuaded for purposes of institution only that Petitioner has shown sufficiently that Peterka in combination with Bocharov, Peterka308, and Chen teaches or suggests the limitations as recited in dependent claims 5 and 15.

IV. CONCLUSION

Based on the arguments and evidence presented by the parties, we determine that there is a reasonable likelihood Petitioner would prevail with respect to at least one claim challenged in the Petition. Hence, we institute an *inter partes* review of all challenged claims on all challenges included in the Petition. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (noting that the language of 35 U.S.C. § 314(b) “indicates a binary choice—

either institute review or don't"); *see also PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018) (interpreting the statute as requiring "a simple yes-or-no institution choice respecting a petition, embracing all challenges included in the petition").

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–7, 9, 11–17, and 19 in the '313 patent is instituted on all challenges included in the Petition;

FURTHER ORDERED that, according to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial that commences on the entry date of this Decision.

IPR2025-00004
Patent 11,122,313 B2

For PETITIONER:

Scott McKeown
Anant Saraswat
Wolf, Greenfield, & Sacks, P.C.
Smckeown-ptab@wolfgreenfield.com
Asaraswat-ptab@wolfgreenfield.com

For PATENT OWNER:

Peter C. Knops
Kayvan B. Noroozi
Noroozi PC
peter@noroozipc.com
kayvan@noroozipc.com