

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner,

v.

ERICSSON AB,
Patent Owner.

Case IPR2025-00004
Patent No. 11,122,313 B2

**PATENT OWNER ERICSSON AB'S
NOTICE OF APPEAL UNDER 35 U.S.C. § 142**

Office of the Solicitor

U.S. Patent & Trademark Office Mail Stop 8
P.O. Box 1450
Alexandria, VA 22313-1450

Submitted Electronically via the PTAB E2E System

Pursuant to 35 U.S.C. §§ 141, 142, and 319, and in accordance with 37 C.F.R. §§ 90.2-90.3, Patent Owner Ericsson AB (“Ericsson”) appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board (“Board”) entered on March 23, 2026, in IPR2025-00004, (Paper No. 42), as to which the Director denied Ericsson’s request for Director Review on July 13, 2026, (Paper 46), and from all underlying findings, determinations, rulings, opinions, orders and decisions regarding the inter partes review of U.S. Patent No. 11,122,313 B2 (the “’313 patent”). A copy of the Board’s Final Written Decision is attached hereto as Exhibit A and a copy of the Order denying Director Review is attached hereto as Exhibit B.

In accordance with 37 C.F.R. 90.2(a)(3)(ii), Ericsson states that the issues on appeal may include, but are not limited to:

- (i) the Board’s determination that Petitioner Google LLC demonstrated by a preponderance of evidence that claims 1–7, 9, 11–17, and 19 of the ’313 patent are unpatentable;
- (ii) the Board’s denial of Ericsson’s Revised Motion to Amend; and
- (iii) any findings or determinations by the Board supporting or relating to the issues above, including without limitation the Board’s claim constructions, the Board’s consideration of expert testimony, prior

art, and other evidence (or lack thereof) in the record, the Board's factual findings, conclusions of law, errors or omissions, or other determinations supporting or related to the above issues, and all other issues decided adversely to Patent Owner in any orders, decisions, rulings, and opinions.

Pursuant to 37 C.F.R. § 90.3, this Notice of Appeal is timely, having been duly filed within sixty-three (63) days after the date of the Order denying Director Review.

This Notice of Appeal is being e-filed with the Clerk's Office for the United States Court of Appeals for the Federal Circuit, along with payment of the required docketing fees. In addition, this Notice of Appeal is being filed simultaneously with the Patent Trial and Appeal Board.

Respectfully submitted,

/s/ Kayvan B. Noroozi

Kayvan B. Noroozi
NOROOZI PC
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025

Date: September 10, 2026

Counsel for Patent Owner

CERTIFICATION OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S NOTICE OF APPEAL** was served electronically via e-mail on September 10, 2026, to the following counsel of record for Petitioner:

Scott McKeown
Anant Saraswat
WOLF, GREENFIELD & SACKS, P.C.
smckeown-ptab@wolfgreenfield.com
asaraswat-ptab@wolfgreenfield.com

Respectfully submitted,

/s/ Kayvan B. Noroozi

Kayvan B. Noroozi
NOROOZI PC
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025

Counsel for Patent Owner

Date: September 10, 2026

Exhibit A

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*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
Denying Patent Owner's Revised Motion to Amend
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, Google LLC (“Petitioner”) challenges the patentability of claims 1–7, 9, 11–17, and 19 of U.S. Patent No. 11,122,313 B2 (Ex. 1001, “the ’313 patent”), which is assigned to Ericsson AB (“Patent Owner”)

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a), addresses issues and arguments raised during the trial in this *inter partes* review. For the reasons discussed below, we determine Petitioner has proven by a preponderance of the evidence that claims 1–7, 9, 11–17, and 19 of the ’313 patent are unpatentable in view of the challenges based on Peterka alone or in combination with Suzuki, Bocharov, Peterka308, and Chen. *See* 35 U.S.C. § 316(e)(2018) (“In an *inter partes* review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.”). We also determine that Patent Owner’s Revised Motion to Amend should be denied.

A. *Procedural History*

Google LLC and Lenovo (United States) Inc. filed the original Petition (Paper 3, “Pet.”) challenging claims 1–7, 9, 11–17, and 19 of the ’313 patent on the following basis:

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 filed a Preliminary Response. Paper 11 (“Prelim. Resp.”). Trial was instituted on the asserted grounds of unpatentability. Paper 13 (“Inst. Dec.”), 42. After trial was instituted, Petitioner Lenovo (United States) Inc. and Patent Owner joined filed a motion to terminate the proceeding as to Lenovo (United States) Inc. only. Paper 17. The motion was granted and Lenovo (United States) Inc. was terminated as a party to the proceeding. Paper 19.

During the trial, Patent Owner filed a Response (Paper 24, “PO Resp.”) to the Petition. In support of its Response, Patent Owner relies on, *inter alia*, the Declaration of John Villasenor, Ph.D. (Dr. Villasenor). Petitioner filed an authorized Reply to Patent Owner’s Response (Paper 30,

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”).

“Pet. Reply”), and Patent Owner filed an authorized Sur-reply to Petitioner’s Reply (Paper 33, “PO Sur-reply”).

Patent Owner filed a contingent Motion to Amend the challenged claims (Paper 23, “PO Motion to Amend”), and Petitioner filed an Opposition to the Motion (Paper 27, “Pet Opp to Motion to Amend”). In accordance with 37 C.F.R. § 42.121(a)(1)(ii), the Board provided preliminary guidance concerning Patent Owner Motion to Amend. Paper 29, “Prelim. Guidance”. Thereafter, Patent Owner filed a Revised Contingent Motion to Amend (Paper 31, “RMTA”), to which Petitioner filed an Opposition (Paper 34, “Opp. RMTA”). In support of its opposition to the Revised Motion to Amend, Petitioner relies on, *inter alia*, the Second Supplemental Declaration of Mr. Wechselberger. Ex. 1047. Patent Owner then filed a Reply to Petitioner’s Opposition (Paper 37, “Reply Opp. RMTA”) and Petitioner filed a Sur-Reply to Patent Owner’s Reply (Paper 39, “Sur-Reply RMTA”). The Revised Motion to Amend states that it is contingent upon a finding that challenged claims are unpatentable. RMTA 1.

An oral hearing was held on January 27, 2026, a transcript of which appears in the record. Paper 41 (“Tr.”).

B. Real Parties in Interest

Petitioner identifies Google LLC as the real parties-in-interest. Pet. 4; Paper 25 (“Petitioner’s Updated Mandatory Notices”).

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.

C. 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.

D. 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:

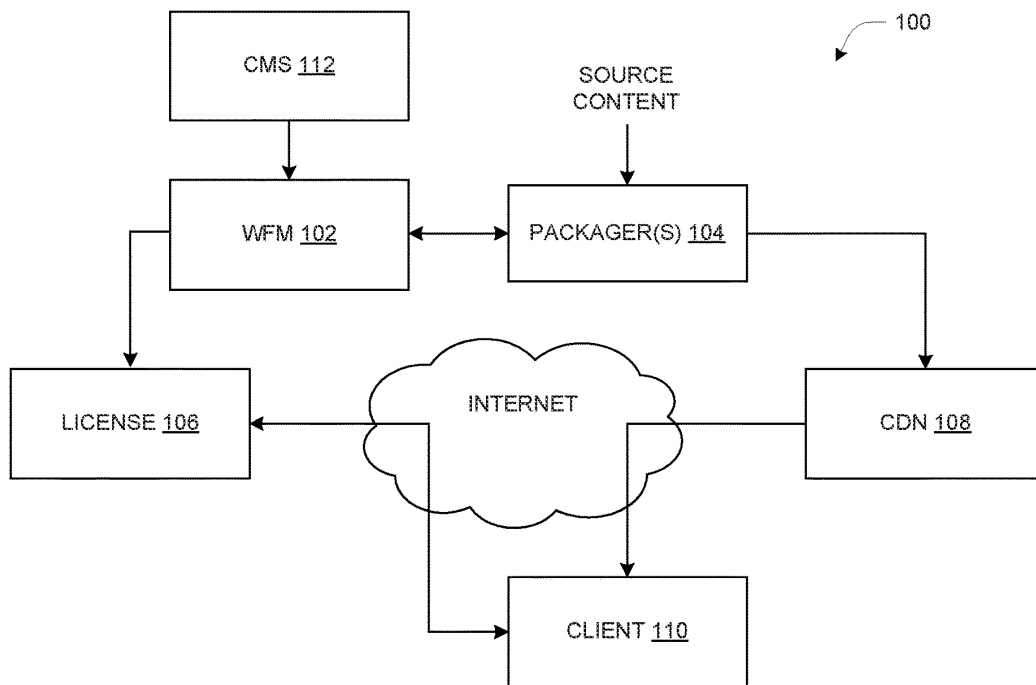


Fig. 1

Figure 1 of the ’313 patent, above, is a block 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.

Another embodiment of the ’313 patent is shown in Figure 3, reproduced below.

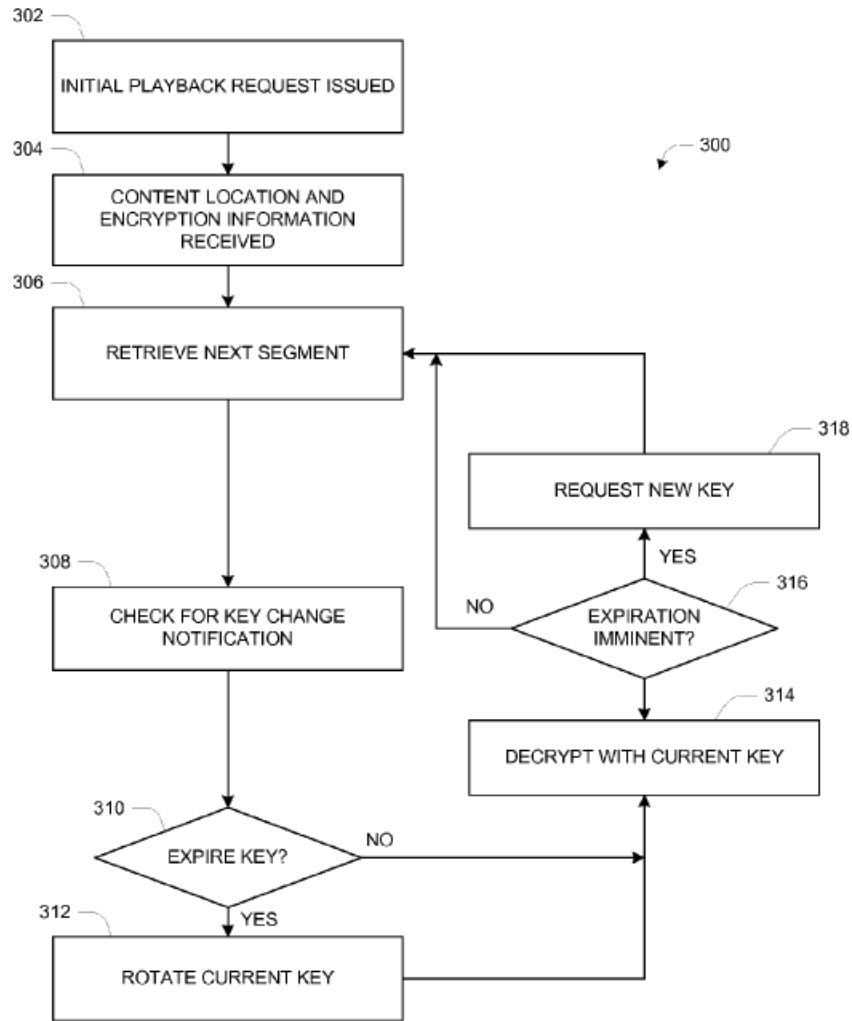


Fig. 3

Figure 3 is a flow diagram showing content downloading and decryption, describing a process for detecting the rotation of content encryption keys and retrieving updated content encryption keys. Ex. 1001, 4:51–52, 9:64–66. After streaming information, including content encryption keys and key expirations, is requested by and received at client 110 in steps 302 and 304, successive segments are retrieved and decrypted in steps 306 and 314. *Id.* at 9:66–10:6, 10:27–43, 11:34–44. During that process, if an encryption key has expired, it is “rotated” — i.e., it is replaced by the next key — in

steps 310 and 312. *Id.* at 1:66–2:6, 11:3–17. Also, during the process, at steps 316 and 318, client 110 checks to see if the current content encryption key is going to expire within a preset time period, and if so, proactively requests a new content encryption key from the license server ahead of time to prevent any latency in or interruption of decryption services.⁶ *Id.* at 11:37–44. There can be content encryption key retrieval failures in step 318, however, in which case in step 312 the client must issue a new content encryption key request to the license server to retrieve the new content encryption key before performing key rotation. *Id.* at 11:17–31. There is also a provision, in step 308, to “check for key change notification,” also described as “check[ing] to see if a key change is signaled,” and “a content encryption key change request is detected.” *Id.* at Fig. 3, 10:57–60, 11:17–21. This is a reference to the above-mentioned occurrence of a key change outside of any fixed duration lifespan for security reasons, in which case the client takes that into account. *Id.*

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):

⁶ Although not specifically disclosed in the specification, Petitioner asserts that at some point after the encryption keys obtained from the initial response in step 304 have been used, subsequent keys are obtained as needed in step 318 from the licensing server. *See* Reply 10; Tr. 24–25.

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.

II. PRELIMINARY MATTERS

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).

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 does not assert an explicit claim construction in its Response, but in its Revised Motion to Amend states that it “does not propose any specific claim constructions.” RMTA 22; *see generally* PO Response.

Nevertheless, the parties’ arguments raise issues regarding the scope of the claims of the ’313 patent, which we discuss below in our analysis of the claims themselves.

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.⁷ *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.

⁷ Patent Owner has not presented objective evidence of non-obviousness.

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 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 agrees with Petitioner’s expert regarding the level of ordinary skill in the art. RMTA 22 (citing Ex. 1003 ¶ 40). Patent Owner’s declarant, Dr. Villasenor, also does not dispute Petitioner’s definition of a person of ordinary skill in the art. Ex. 2010 ¶ 19. Dr. Villasenor notes, however, that “obviousness must be viewed from the perspective of one of

ordinary skill in the field of information security using cryptographic keys for encryption and decryption of digital data, and my opinions are rendered on the basis of the definition of the ordinary artisan set forth in the Petition in view of that further clarification.” *Id.*

For our analysis, 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. We note that applying Dr. Villasenor’s “clarification” does not change our analysis.

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, which depicts the free preview approach, and is reproduced below.

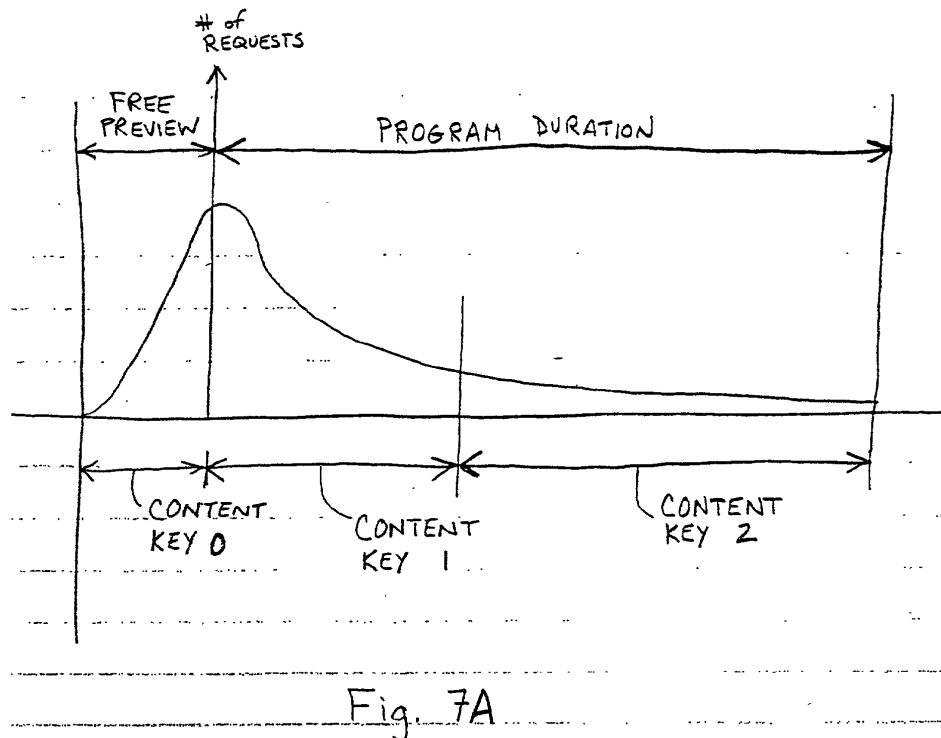


Figure 7A of Peterka, above, is “a plot showing the number of requests for a program versus the program duration.” Ex. 1005 ¶ 91; *see also id.* ¶ 21 (“showing exemplary distribution of cryptographic keys during portions of a program”). Peterka explains that “an initial free preview period provides for 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.*

Another embodiment of Peterka is shown in Figure 7B, reproduced below.

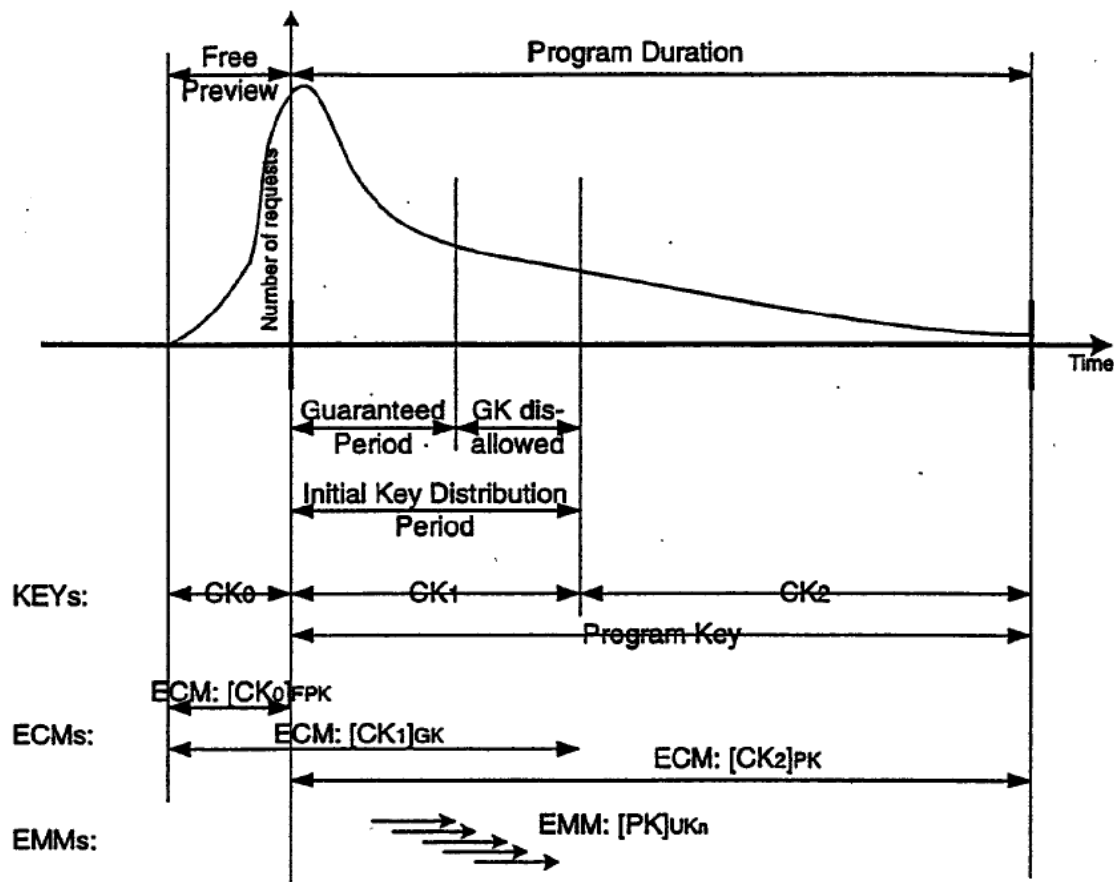


Fig. 7B

Figure 7B is a more detailed version of Figure 7A showing distribution of Content Keys during portions of a program, in which the Content Keys are

distributed via “Entitlement Control Messages” (ECMs), which are multicast to a group of authorized clients that have “higher level keys.” Ex. 1005 ¶¶ 21, 104, Table 1. In particular, in the specific example of Figure 7B, an ECM sends the Content Key CK_0 for the “free preview period” encrypted with a “Free Preview Key” (FPK), the latter which can be provided in advance to the group of authorized clients via “provisioning.” *Id.* ¶¶ 85, 103, 122. At the same time that the ECM for CK_0 is sent, another ECM sends the Content Key CK_1 encrypted with a “Group Key” (GK), which key is used for the “initial key distribution period,” also called the “initial viewing period.” *Id.* ¶¶ 90, 102, 122, 127, 130. Like the FPK, the Group Key can also be provided in advance to the group of authorized clients via provisioning. *Id.* ¶ 102. For the remainder of the program that takes place after the initial viewing period, a third ECM sends the Content Key CK_2 encrypted with a “Program Key” (PK), which is used to give access to paid content. *Id.* ¶¶ 98, 122. As shown by the multiple short arrows at the bottom of the figure, each client that pays for the program after the free preview period receives the Program Key encrypted with their “Unique Key” via an “Entitlement Management Message” (EMM), which is a unicast message to deliver keys to individual clients. *Id.* ¶¶ 104, 122.

Peterka describes various models for distributing keys to clients. Ex. 1005 ¶ 105. For example, Peterka describes a “Pull” or “Pay-By-Time” (PBT) 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).

For the PBT content purchasing option, in which the client pays for the time duration of the content that was actually watched, which could

apply, for example, to sporting and music events. Ex. 1005 ¶¶ 53, 78. The program content is divided into purchasable segments and encrypted with separate segment keys for each segment. *Id.* ¶¶ 53, 80, 99. In particular, Content Keys are provided to the client to allow the client to decrypt the segments of the encrypted program material. *Id.* ¶¶ 6, 101. One way of distributing Content Keys is to encrypt each content key with a “Program Segment Key” (PSK), which is distributed for each purchasable segment. *Id.* ¶¶ 99, 116. 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.*

The fact that the above specific example of Figure 7B encrypts CK2 with a Program Key, and uses a single CK2 for the remainder of the program, indicates that this specific example pertains to a “Pay-Per-View” (PPV) program, because program keys are used for the Pay-Per-View option, and Pay-Per-View programs are not divided up into a sequence of separately encrypted segments. Ex. 1005 ¶¶ 52, 98, 92, 105, Table 1. However, disclosures in Peterka establish that the free preview/initial viewing approach is also applicable to the above-described Pay-By-Time purchasing option, where, after the free preview and initial viewing periods, a series of purchasable segments encrypted with separate Content Keys are multicast, with ECMs sending the Content Keys encrypted with Program Segment Keys rather than Program Keys:

Yet another alternative [for Free Preview] is to distribute a Program Segment Key (PSK) that is encrypted with FPK. The PSK is then utilized to deliver the content key encrypted with PSK. *Id.* ¶ 87.

Clients will get the GK ahead of program events sold on PPV or PBT basis, for instance during provisioning. That will give the viewer the option to watch the beginning of the content while the client negotiates the other key(s) with the caching server. *Id.* ¶ 102.

Thus, when a multicast event starts the initial content key can be distributed under the group key as well as the program key for pay per view events *or a first program segment key for pay by time events (the PSK can be encrypted under the GK, as well)*. *Id.* ¶ 128 (emphasis added)

In the discussion of requesting access to paid content during the Initial Viewing Period of Figure 7B: “delivery of the program key *or program segment key*.” *Id.* ¶ 132 (emphasis added).

Accordingly, adapting Figure 7B to the Pay-By-Time option would substitute references to Program Keys with Program Segment Keys, which would be sent via Entitlement Management Messages to clients that are paying for the program. *Id.*

Generally, Entitlement Control Messages and Entitlement Management Messages sent to clients include, in addition to the encryption code, a sequence number or a time stamp to protect against replay attacks, an identification of the type of key included in the message and the type of key used to encrypt the key in the message, and the time remaining in the lifetime of the key. Ex. 1005 ¶ 121.

Disclosed embodiments, applicable to the Pay-By-Time option or “pull model,” in 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.” Ex. 1005 ¶ 105, *see also* ¶ 80 (“[E]ach [client] is given keys to the current as well as the next segment”), ¶ 82 (“The client will monitor the expiration time for each pay period and request a new set of keys from the caching server”), ¶ 106 (“The pull key distribution model allows each client to actively request keys from the server the server need not monitor the status of the client's keys; rather, the responsibility of determining when a new key is required can be passed to the client”), ¶ 114 (“[The client] can monitor the expiration time of the program segment key and send an individual key update request before the key expires”), ¶ 130 (“the next content key will have been obtained by a purchasing user prior to the initial key distribution period elapsing”).

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.

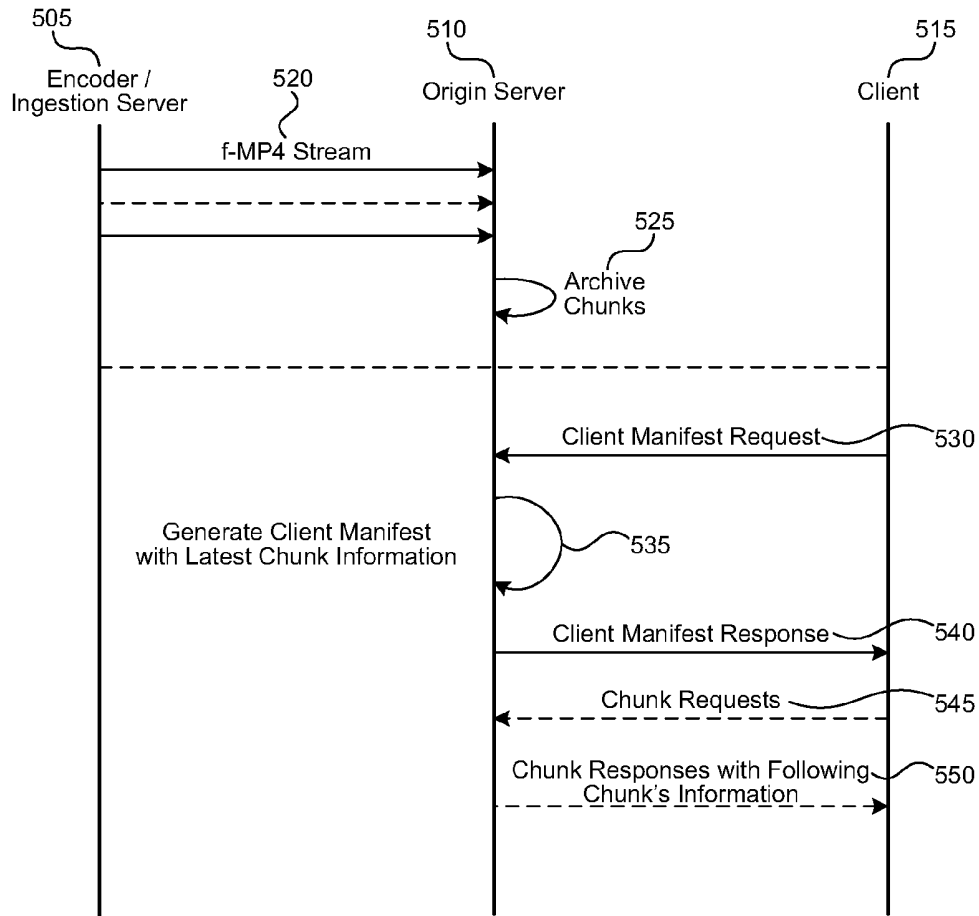


FIG. 5

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. PO Resp. 6–40; PO Sur-Reply 1–20. Patent Owner specifically challenges whether Petitioner has shown that Peterka alone or with Suzuki teaches limitations ([1A]) “sending a request for live media playback” and ([1B]) “receiving a live media playback request response comprising content encryption keys and content encryption key identifiers,” as required by challenged independent claims 1 and 11. PO Sur-Reply 1. Patent Owner further challenges whether Petitioner has demonstrated a reason to combine Peterka with Suzuki. PO Resp. 40.

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 agree with Petitioner’s contentions regarding the preamble, and therefore, we need not determine whether the preamble is limiting.

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:

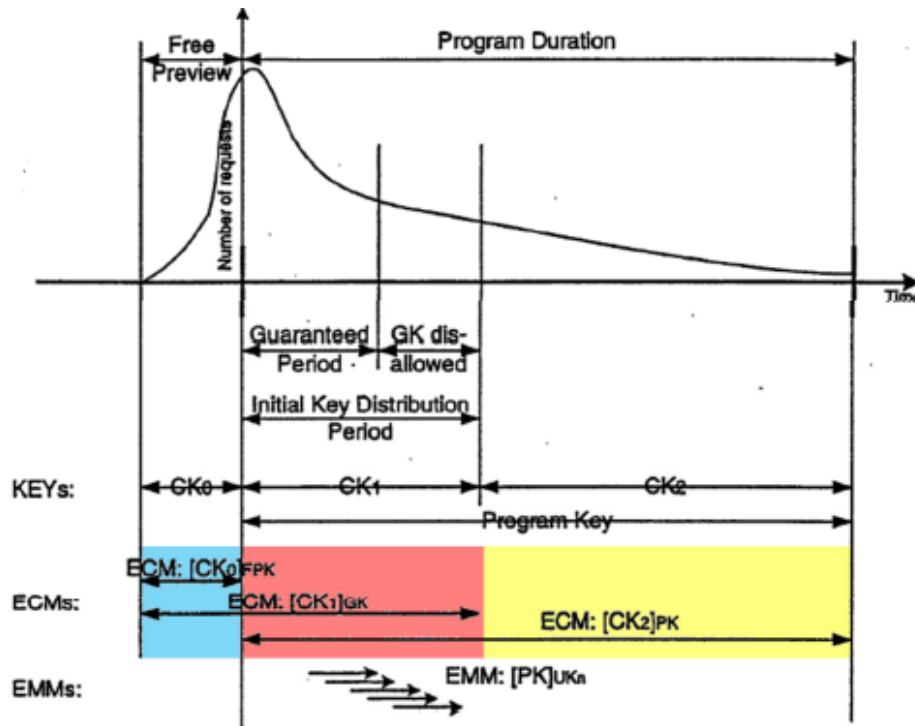


Fig. 7B

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 contends the claims require that one request is sent and that in one response there must be multiple content encryption keys. PO Resp. 6–7 (citing Pet. 21–23; Ex. 1003 ¶¶ 81, 84). In this section, we only address whether the prior art teaches whether a single request is sent and whether a single response is received in response as required by the claims.

Based on the entire trial 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 find 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 that disclosure 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. Petitioner argues that the playback request response of Peterka includes multiple keys and associated information. *Id.* at 19–22, 23, 27 (citing Ex. 1005, Fig. 7B, ¶¶ 21, 53, 79–80, 121, 130; Ex. 1003 ¶¶ 77–79, 100). In particular, Petitioner relies on the Pay-By-Time disclosure that “each [client] is given keys to the current as well as the next segment.” *Id.* at 19 (citing Ex. 1005 ¶ 80); *see* Ex. 1003 ¶ 77); *see also* Ex. 1005 ¶ 100 (“[t]wo PSKs are distributed at any given time: the current PSK and the next one”), ¶ 130 (“the next content key will have been obtained by a purchasing user prior to the initial key distribution period elapsing”). Petitioner also relies on the Figure 7B illustration of multiple keys being sent: “two content keys CK₀ and CK₁ distributed in separate ECMs for each request received during a free preview period . . . and two content keys CK₁ and CK₂ distributed in separate ECMs for each request received during an initial key distribution period” Pet. 20–22 (citing Ex. 1005, Fig. 7B, ¶¶ 21, 53, 79–80, 121, 130; Ex. 1003 ¶¶ 78–79); *see* Reply 4.⁸

⁸ The parties agree that the fact that separate messages are relied on, if in response to one request, is not itself a disqualification for satisfying the claims. Pet. 21–22; PO Resp. 31–32.

Patent Owner specifically construes this limitation to mean that “the playback request response” must comprise *multiple* “content encryption keys.” PO Resp. 6. According to Patent Owner, the Petition agrees with this interpretation. *Id.* at 6–7 (citing Pet. 21–23; Ex. 1003 ¶¶ 81, 84). Patent Owner notes that the ’313 patent states, “In one embodiment, when initiating playback of the stream, the client requests the current content encryption key [and] the next future content encryption key” *Id.* at 3 (citing Ex. 1001, 3:56–61). Patent Owner then argues that there is no teaching or suggestion in Peterka of providing more than one encryption key in response to a request for program content. *Id.* at 9 (citing Ex. 2010 ¶ 29).⁹

Focusing on Petitioner’s reliance on the free preview/initial viewing approach of Figure 7B as implemented for the Pay-By-Time purchasing option,¹⁰ Patent Owner argues that neither the CK₀ and CK₁ keys sent during the free preview period nor the CK₁ and CK₂ keys sent during the initial viewing period are sent in response to any playback request, as required by claim 1. PO Resp. 14–23, 26–29 (citing Ex. 1005, Figs. 7A, 7B, ¶¶ 9, 53, 59, 81, 83–85, 90–93, 102–103, 122, 126–128, 131, 133; Ex. 2010 ¶¶ 44, 50–53, 59, 63). Patent Owner explains that CK₀ and CK₁ are provided in advance, during a “provisioning” process, before there is any playback request or response. *Id.* at 20–21. Patent Owner submits that the only key in Figures 7A and 7B that is requested is CK₂, which is delivered only to those

⁹ Exhibit 2010 is the Declaration Of John Villasenor, Ph.D. In Support Of Patent Owner’s Response.

¹⁰ Patent Owner discusses in detail other embodiments and aspects of Peterka, which we need not discuss because Petitioner does not rely on them. *See* PO Response 9–14; Reply 5–8.

clients that purchased the content. *Id.* at 22–23, 26–27 (citing Ex. 1005, Figs. 7A, 7B, ¶¶ 92–93, 129–131; Ex. 2010 ¶¶ 54, 59).

Patent Owner also argues that Petitioner’s reliance on the “pull” model in Peterka is insufficient, because the pull model only provides one content key in response to each client request. PO Resp. 9, 23–26 (citing Ex. 1005, Fig. 8, ¶¶ 106, 110, 114; Ex. 2010 ¶¶ 30, 55–58). In response to Petitioner’s reliance on the statement in Peterka that, for the Pay-By-Time option, “each [client] is given keys to the current as well as the next segment” (at Ex. 1005 ¶ 80), Patent Owner argues that this passage merely discloses that each pull request provides only one content key, but timed to arrive before the prior key expires to avoid service interruptions — thus the client has two content keys during a given segment — the previously-requested key for the current segment and the currently-requested key for the next segment. *Id.* at 27–28 (citing Ex. 2010 ¶¶ 59, 60). For the same reason, Patent Owner challenges Petitioner’s reliance on other similar statements in Peterka. *Id.* at 28–32 (citing Ex. 1005 ¶¶ 53, 101, 105, 130–131; Ex. 2010 ¶¶ 62, 64–65). Patent Owner further argues that Petitioner has not demonstrated that it would have been obvious to an ordinary artisan “to package multiple keys/entitlement messages (ECMs or EMMs) into a ‘single’ ‘combined’ ‘multicast message,’” *Id.* at 31–36 (citing Pet. 21–22, 25–26; Ex. 2010 ¶¶ 66–77).

Petitioner in reply reiterates its argument that, for the requirement that the playback response provides multiple encryption keys, Petitioner relies on the Peterka “key management approach” where clients are given keys to both the current and next segments of media to mitigate server load at segment boundaries. Reply 3 (citing Pet. 19–22; Ex. 1005, Fig. 7B; Ex. 1003 ¶¶ 76–78). Petitioner further argues that Peterka Figures 7A and

7B are a confirmation that the “‘key management approach’ of ‘distributing multiple keys (e.g., current and next) to a client when it negotiates access to media content’ was both ‘applicable’ and ‘*desirable* in any distribution scheme in which key requests from many clients are expected at segment boundaries.’” *Id.* at 7–8 (citing Pet. 20–22; Ex. 1003 ¶ 78). Petitioner asserts that this “would predictably reduce the volume of requests that the server needed to respond to ahead of the upcoming segment boundary and help reduce disruptions in content distribution due to latency caused by any network congestion that arises from many clients using the network to transmit requests.” *Id.*

Petitioner contends that Patent Owner’s argument that Peterka fails to teach or suggest a “*client-initiated content key request*” misreads the claim requirement—claim 1 only requires a client to “initiat[e] a media playback request,” it “*does not require* the media playback request *to include any specific data*, e.g., a specific request for a [content encryption code].” Reply 8–9 (citing PO Resp. 16–17, 20–22). Rather, Petitioner asserts that “the claim encompasses precisely what is taught in Peterka: a client that initiates a media playback request and receives multiple content keys in response, and then pulls additional content keys from a license server during playback.” *Id.* at 10 (citing Pet. 18–21, 25–26, 32).

In addition, Petitioner argues that Patent Owner’s argument that the CK₀ and CK₁ encryption codes of Figures 7A and 7B are “provisioned” or otherwise provided in advance before there is any media playback request is a mischaracterization of Peterka. Reply 10–15. To the contrary, argues Petitioner, “Peterka never once discusses ‘provisioning’ keys ‘ahead of time’ in the context [of] CK₀ and CK₁,” and “Peterka does not even identify ‘provisioning’ as an option for ‘content keys.’” *Id.* at 12 (citing Ex. 1005,

Table 1, ¶¶ 83, 85, 102–104, 122–125, 127–130). Petitioner submits that Peterka itself states that Figure 7B “show[s] exemplary distribution of cryptographic keys *during portions of a program*,” and Figure 7B specifically shows transmission of ECM messages containing the CK₀ and CK₁ keys during content requests. *Id.* at 12–15 (citing Ex. 1005, Fig. 7B, ¶¶ 21, 91, 122; Ex. 1003 ¶ 78). Petitioner argues that the only keys that are “provisioned” in advance of content requests are keys used in alternatives to Figure 7B that are not relied on by Petitioner. *Id.* at 15.

Petitioner also contends that Patent Owner misleadingly argues that Petitioner’s reliance on the pull model of Peterka does not teach the claim requirement of obtaining multiple encryption keys from the playback request response, when in fact Petitioner relies on the pull model for other requirements of the claim regarding key distribution which occurs after a request to access media content has been initiated and the first set of content keys have already been negotiated/received. Reply 15–16.

Patent Owner disagrees and argues that Petitioner’s reliance on the description of the key management approach for the Pay-By-Time option where “each [client] is given keys to the current as well as the next segment” is insufficient because it “does not state that multiple content keys (one for the current segment and one for the next) are provided in response to a single ‘playback request,’ as [the claims] require.” Sur-Reply 1–2, 5, 13 (citing Ex. 1005 ¶ 80). Rather, according to Patent Owner, Peterka states that only one key is requested during a segment, which key is for the next segment. *Id.* at 2.

Patent Owner reiterates its argument that the only client-initiated request for media playback for the Pay-By-Time option is “when a client *purchases* the right to view a pay-by-time content segment.” Sur-Reply 3–4

(citing Ex. 1005, Fig. 7B, ¶¶ 93, 129–131; Ex. 2010 ¶ 53). Patent Owner asserts that Pay-By-Time embodiments in which media and keys are provided before the clients have made a purchase decision are provided without any client request. *Id.* at 4, n.1 (citing PO Resp. 14–22).

Patent Owner focuses on a statement by Petitioner that “[e]very *element* of claims 1 and 11 is satisfied by or obvious over Peterka’s *pull* method,” but, argues Patent Owner, for the pull method of Peterka “each client receives only *one* content key in response to each client request for media.” Sur-Reply 4–6 (citing Pet. 18; Ex. 1005, Fig. 8, ¶110; Ex. 2010 ¶¶ 54–56). Patent Owner argues that Petitioner’s Reply arguments improperly attempt to change its arguments to avoid this reliance on the pull method. *Id.* at 5–6.

Patent Owner also asserts that Petitioner changed its reliance on Peterka Figure 7B in the Reply, and argues that the Petitioner mischaracterized Peterka’s teachings as to that figure, because, according to Patent Owner, CK₀ and CK₁ of Figure 7B are each distributed without any request from the client. Sur-Reply 8–9. Patent Owner argues that “the ***Petition’s theory*** relies on a client-initiated request for content under the pay-by-time model using the pull distribution method, but this theory cannot meet what the claims expressly require.” *Id.* at 9.

Regarding CK₀ and CK₁ of Figure 7B, Patent Owner points out that those keys are “packaged under the free preview key (FPK) and . . . group key (GK),” and reasons from the fact that because the FPK and GK are provisioned in advance, then so are CK₀ and CK₁, and therefore CK₀ and CK₁ cannot be provided in response to a client request. Sur-Reply 9–11 (citing Ex. 1005, Fig. 7B, ¶¶ 85, 102–103, 122). Patent Owner also asserts that Petitioner mischaracterizes the import of the graph of the “number of

requests” in Figure 7B, because the “requests” referred to are requests to purchase content, not requests for free preview. *Id.* at 12. Furthermore, Patent Owner argues that the fact that the ECM messages that contain the CK₀ and CK₁ keys are shown as being transmitted at the point in time where the graph shows that no requests haven yet been made, demonstrates that those keys are no sent in response to a request. *Id.* at 11–13.

First, we disagree with Patent Owner’s assertion that Petitioner raises new arguments in its Reply. Rather, Petitioner has relied consistently on the teachings of Peterka that involve both the disclosures regarding the “pay-by-time” purchasing option with a “free preview” offer, together with the “pull model” of encryption key distribution. Pet. 10–12, 19–28, 31–36; Reply 3–17, 23–27. As Petitioner explains:

Peterka discloses both receiving keys in response to a request to access media content . . . and then “pulling” keys on an ongoing basis during playback In Peterka and in the Petition, reference to the “pull” model refers to key distribution . . . which, e.g., occurs *after* a request to access media content has been initiated and the first set of content keys have already been negotiated/received

Reply 16. In particular, we find Petitioner relies on the pay-by-time purchasing option, in which two encryption keys — CK₀ and CK₁ — are provided during a free preview period, then followed by a sequence of pay segments with each successive individually assigned key obtained under the pull method before the current key expires.¹¹ Ex. 1005, Fig. 7B, ¶¶ 80–82. This tracks the disclosed embodiment of the ’313 patent, in which the initial request for playback provides the current content encryption key and the

¹¹ Figure 7B of Peterka only shows one key (CK2) for one paid segment, but as discussed in Section III.D.1 above, the pay-by-time option involves a succession of paid segments, each with its own key.

next future content encryption key, followed by successive requests for subsequent keys before key rotation boundaries occur. *Id.* at Fig. 3, 3:62–66.

Second, we also find that Patent Owner mischaracterizes Figure 7A and 7B of Peterka, asserting that the CK₀ and CK₁ keys shown in the figures are provisioned in advance, rather than sent as a result of a media playback request. *See* PO Resp. 16. However, as Petitioner asserts, and as Figure 7B explicitly shows, CK₀ and CK₁ are sent via ECM messages during the free preview period, not at some prior “provisioning” time. Reply 7. Moreover, Patent Owner provides insufficient evidence for asserting that the ECMs that are sent during the free preview period are not sent in response to a request. Peterka explains that the pay-by-time option and free preview period are “offered,” and that such offers then allow a client to “make a decision” or “selection.” Ex. 1005 ¶¶ 59, 81, 93, 144–145. Such decisions or selections are not limited to deciding or selecting to purchase content, they also reasonably encompass deciding or selecting to accept a free preview period. Patent Owner appears to assume that a free preview simply occurs due to some unknown agency without any client request — yet there is insufficient support in Peterka for that speculation.

Third, we are not persuaded by Patent Owner’s argument that Petitioner’s reliance on the statement in Peterka, “each [client] is given keys to the current as well as the next segment” (at Ex. 1005 ¶ 80), does not support the multiple content encryption keys requirement. In the context of Figure 7B, we find that statement supports the fact that CK₀, which is key for the initial free preview period, and CK₁, the key for the subsequent initial viewing period, are both sent in response to a single request. Patent Owner’s interpretation of that passage, asserting that it only refers to pull requests that

provide a single content key, at most applies to the subsequent period of key distribution, after the free preview and initial viewing periods, in which the pull method is applied to successive keys during the viewing of paid content.

Accordingly, we determine that at least the disclosure of Figures 7A and 7B, in the context of the pay-by-time option, in which both CK₀ and CK₁ are provided during a free preview period, satisfies the claim requirement of a playback request response that includes multiple “content encryption keys.”

(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.” PO Resp. 36–43. Patent Owner argues that the content encryption key identifier “must be ‘*unique*’ in the context of *all* content encryption keys maintained in the ‘history’; and “each content encryption key identifier must be ‘assigned’ to the corresponding content encryption key itself.” *Id.* at 36–37 (citing Ex. 2010 ¶¶ 81–82). Patent Owner bases this on the statement in the ’313 patent:

A history of individual content encryption keys and the order in which they were generated is maintained. Each content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier.

Id. at 36 (citing Ex. 1001, 3:36–40).

Patent Owner argues that Peterka’s sequence numbers or time stamps that Petitioner relies on “are only assigned to its ECM/EMM *messages*, and not the content key included in those messages,” and therefore are message identifiers rather than key identifiers and “cannot meet the challenged claims.” PO Resp. 38–39 (citing Ex. 1005 ¶ 121; Ex. 2010 ¶¶ 79–82, 88).

Patent Owner also argues that Petitioner has not demonstrated that it would have been obvious in light of Peterka to provide identifiers that were specifically assigned to encryption keys. PO Resp. 39–42. Patent Owner submits that the fact that Figure 7B of Peterka individually labels keys CK₀, CK₁, and CK₂ does not suggest sending such labels to clients as key identifiers. *Id.* at 40 (citing Ex. 2010 ¶ 93). Patent Owner also argues that the fact that Peterka uses unique message identifiers that each carry a single

key negates any motivation to add specific key identifiers to the Peterka system. *Id.* at 40–41 (citing Ex. 2010 ¶¶ 94–96).

Petitioner argues that Patent Owner’s proposed construction of the encryption key identifiers requirement, that the identifier “must be ‘*unique*’ in the context of *all* content encryption keys maintained in the ‘history’; and “each content encryption key identifier must be ‘assigned’ to the corresponding content encryption key itself,” is nowhere to be found in the claims and is an improper attempt to import descriptions from the specification into the claims. Reply 20–21. Petitioner submits that there is no definition or disavowal of coverage in the specification that would justify Patent Owner’s construction. *Id.* at 21. Petitioner also cites the fact that the sequence number or time stamp of the ECM messages of Peterka closely tracks the use of segment numbers as the key identifiers in the ’313 patent. *Id.* at 21–22 (citing Ex. 1001, 3:43–45, 4:17–19).

Furthermore, Petitioner argues that the relied-on sequence numbers and time stamps are sufficient to uniquely identify the associated keys and relies on its declarant’s testimony citing background art in support. Reply 22 (citing Ex. 1003 ¶¶ 91–94, 151–161, 187–192, 194–220; Ex. 1041 ¶¶ 239–242; Ex. 2011, 39:7–40:13). Petitioner urges the Board to reject Patent Owner’s arguments against the obviousness of using specifically assigned unique identifiers given Patent Owner’s acknowledgement that there is no meaningful difference between using Peterka’s sequence numbers/time stamps as identifiers for individual keys and specifically assigning identifiers to individual keys. *Id.* at 22–23 (citing PO Resp. 40–42).

Patent Owner the replies that the statement in the ’313 specification, “[e]ach content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier,” is a

definition of “encryption key identifier” — *i.e.*, “constitutes lexicography” — given the use of the phrase “referred to herein.” Sur-Reply 17 (citing Ex. 1001, 3:38–40; *Kyocera Senco Indus. Tools Inc. v. Int’l Trade Comm’n*, 22 F.4th 1369, 1378 (Fed. Cir. 2022)). Patent Owner also argues that the Peterka ECM sequences numbers and time stamps are not uniquely assigned to a content key within that ECM because the ECMs carry multiple keys. *Id.* at 19.

In addition, Patent Owner challenges Petitioner’s reliance on the Figure 7B key identifiers, CK₀, CK₁, and CK₂, as rendering the encryption key identifier requirement obvious, arguing that they are “merely *descriptive labels* provided in Peterka’s written description for purposes of explanation and illustration.” Sur-Reply 20.

(b) *Analysis of Peterka*

Based on the entirety of the trial record, we agree with Petitioner. 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 CK₀, CK₁, and CK₂, without the

requirement that the identifier actually being tied directly to the key itself. *See* Ex. 1005 ¶ 122, Figs 7A, 7B.

We determine that the disclosure in Peterka that EMM and ECM messages include “a sequence number or a time stamp to protect against replay attacks,” satisfies the claim requirement that a playback request response include “content encryption key identifiers.” Patent Owner relies on the statement on the ’313 patent that “[e]ach content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier.” *See* PO Resp. 3 (citing Ex. 1001, 3:38–40). Immediately after that statement, however, the patent further states:

In one embodiment, the content encryption key identifiers are selected based on the wall clock time offset from the beginning of the live stream. In another embodiment, the content encryption key identifiers are selected based on a segment number of the prepared content.

Ex. 1001, 3:40–45. We do not see how Peterka’s “sequence number or a time stamp” differs in any pertinent respect from the ’313 patent’s “wall clock time” or “segment number.” Likewise, we do not agree that simply because Peterka includes the sequence number or time stamp in the EMM or ECM message along with the key this somehow fails to satisfy the ’313 patent’s description that the identifier is “assigned” to the key. In particular, we reject Patent Owner’s assertion that more than one key is included in the EMM and ECM messages. *See* Sur-Reply 19–20. There is simply no basis for that assertion. The fact that CK_0 is encrypted with the FPK key and CK_1 is encrypted with the GK key does not support Patent Owner’s assertion.

(c) *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.” PO Resp. 35–36. First, Patent Owner contends that “Suzuki’s paragraphs 76 and 77 do not teach transmitting multiple “*content encryption keys*,” they only disclose providing “key *information* relating to the key currently in use (key A) and the next key to be used (key B).” *Id.* at 35 (citing Ex. 1006 ¶¶ 76-77; Ex. 2010 ¶ 77). According to Patent Owner, “Suzuki is not directed to a pay-by-time, pay-per-view, or subscription distribution model, in which a content key grants access to content that different clients must individually decide to purchase in discrete units or increments, as in Peterka.” *Id.* (citing Ex. 2010 ¶ 77). Therefore, Patent Owner asserts “Suzuki could not motivate providing Peterka’s clients with unpurchased content for segments or subscription periods that were designed to require a purchase.” *Id.* at 35–36.

Patent Owner next contends that “Petition likewise defeats its own motivation as to the combination of Peterka and Suzuki. PO Resp. 40 (citing Pet. 46–47 (contending “[a] POSITA would have recognized the importance of [key] 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.”)). Patent Owner asserts that if Peterka’s message identifiers already serve that purpose, then there would be no motivation to add key identifiers because Peterka does not need to solve a problem it does not have. *Id.* at 40–41 (citing Ex. 2010 ¶ 94).

As explained previously, we agree with Petitioner’s position regarding Peterka. Specifically, Peterka’s teachings 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) is 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) is 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).

We also find based on the complete trial 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 find 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). Therefore, crediting the

testimony of Mr. Wechselberger, find 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 all the arguments and evidence, we find 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 agree with Petitioner 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* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed Peterka, on the complete trial 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, we find 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* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed Peterka, on the complete trial 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 find 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 find 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 determine 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* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed the entirety of the trial record, we find 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* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed the entirety of the trial record, we find 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* PO. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Having reviewed the entirety of the trial record, we find 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.

g) Summary of Analysis of Independent Claim 1

Based on the above analysis, on our complete review of Peterka’s disclosures regarding the requirements of claim 1, and having considered and weighed the entirety of the evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 1 is unpatentable under 35 U.S.C. § 103(a) over Peterka alone or in combination with Suzuki.

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.

Other than its arguments directed to Petitioner’s challenges to the independent claim 1, Patent Owner does not specifically respond to Petitioner’s arguments regarding independent claim 11 and dependent claims 2–4, 6, 7, 12–14, 16, and 17. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Independent claim 11 a system claim directed to implementing the method of claim and includes a computerized device, a memory, and processors for operating computer program instructions from memory that cause the device to perform the recited operations, which are similar to those recited in independent claim 1. *See* Ex. 1001, 13:9–39. For the same reasons regarding claim 1, we determine that Petitioner has proved by a preponderance of the evidence that claims 11 is unpatentable under 35 U.S.C. § 103(a) over Peterka alone or in combination with Suzuki.

Claims 2 and 12 a first content encryption key and associated identifier as well as a second content encryption key and associated identifier. *See* Ex. 1001, 12:45–48, 14:1–5. We find that Peterka teaches a client receiving multiple content encryption keys—for a current (first) and next (second) segment, each in one ECM/EMM—and identifiers for those keys (associated identifiers). *See* Ex 1005 ¶ 80 (“keys to the current as well as the next segment”), ¶ 130, Fig 7B.

Claim 3 and 13 require content encryption key rotation boundaries that are expressed as an expected minimum interval between boundaries. *See* Ex. 1001, 12:49–51, 14:6–8. We find that Peterka teaches media streams that are divided into “purchasable segments” to allow users to pay according to the amount of time—e.g., number of segments—that the user consumes. *See* Ex 1005 ¶¶ 78–82, 99–101. Peterka further teaches that each segment is encrypted by a different content key. Peterka also indicates that segments having a defined period and keys for those segments being periodically rotated at regular intervals. *Id.* ¶¶ 81–82, 110. Petitioner asserts, and we agree, that the key expiration times in Peterka’s ECMs/EMMs correspond to the key rotation boundaries found in Peterka’s encrypted live media content stream, because each expiration time describes when a key used to encrypt data in the encrypted live media content stream changes—i.e., the *boundary* between the use of one key and the next. *See* Pet. 35–36 (citing Ex. 1003 ¶ 122; *cf.* Ex. 1001, 7:42–46). We credit the testimony of Dr. Wechselberger who testifies that an ordinarily skilled artisan would have understood that each of Peterka’s ECMs/EMMs includes a field that *expresses the content encryption key rotation boundaries* found in Peterka’s encrypted live media content stream as *intervals*. *See* Ex. 1003 ¶ 122. We credit Dr. Wechselberger’s additional testimony and find that an ordinarily skilled artisan would also have understood that the remaining time in the key’s lifetime described in Peterka constitutes a “*minimum interval*” that the key in the ECM/EMM is “*expected*” to be used “*between boundaries.*” *Id.* ¶ 123 (citing Ex. 1005 ¶ 121).

Claims 4 and 14 require obtaining a third content encryption key at a fixed duration before the expected expiration of the second content encryption key. *See* Ex. 1001, 12:52–54, 14:9–14. We find an ordinarily

skilled artisan would have understood that Peterka’s pay-by-time distribution scheme teaches the claim limitation because a client requests and receives encryption keys on an ongoing basis to gain access to segments of an ongoing media stream and makes those ongoing requests a *fixed duration* before expiration of the current key. *See* Ex. 1005 ¶¶ 80–82, 105–106.

Claims 6 and 16 require license server communications to be secured and authenticated using a selected one of Secure Sockets Layer and a token-based technique using a token encrypted with a symmetric key. *See* Ex. 1001, 12:58–61, 14:18–21. We find Peterka teaches a “token-based technique” because Peterka discloses securing communications between clients and license servers by requiring clients to present a security “ticket” to the server when requesting access to content or fetching keys from the server. *See* Ex. 1005 ¶¶ 66, 75, 136, 142–144, Figs. 19–21. Peterka also explains that the ticket or similar data is “authenticated and encrypted so that the client cannot revise his own entitlements.” *Id.* ¶ 146, Fig. 23. We credit the testimony of Dr. Wechselberger who testifies that an ordinarily skilled artisan would have reasonably expected success implementing Peterka to use symmetric keys to encrypt its client ticket (or other token). *See* Ex. 1003 ¶ 139.

Claims 7 and 17 require that the content encryption key rotation boundaries comprise real-time inband notifications. *See* Ex. 1001, 12:62–64, 14:22–24. We find that Peterka discloses including a signal in the content stream that informs a client of key changes. *See* Ex. 1005 ¶¶ 116–121, Fig. 14. We specifically find that Peterka teaches using “a predetermined bit” in the content stream “to indicate if an old or current content key should be used as opposed to a new content key which has

recently been distributed to the client.” *See id.* ¶ 117. We credit Dr. Wechselberger’s testimony explaining that Peterka’s signals in the content stream that indicate that a key has changed are *content encryption key rotation boundaries* as claimed, because one key must be used for decryption before the signal, and another key must be used for decryption after the signal. Ex. 1003 ¶ 142. We also find similar to that disclosed in the ’313 patent, Peterka’s signals “comprise *real-time in-band notifications*,” because the signals are embedded in Peterka’s content packets (*inband*) and occur at the time the client needs to switch keys for decryption (*in realtime*). *See* Ex. 1001, 4:22–24.

Having reviewed the entire trial record, we find that Petitioner has shown that Peterka alone or in combination with Suzuki teaches or suggests the limitations as recited in dependent claims 2–4, 6, 7, 12–14, 16, and 17. Accordingly, we determine that Petitioner has established by a preponderance of the evidence that claims 2–4, 6, 7, 12–14, 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” and “content encryption key identifiers” limitations. *See* PO Resp. 40–42. Patent Owner argues that an ordinary artisan could not have been motivated to modify Peterka to better manage multiple content keys obtained multiple segments in advance. *Id.* (citing Ex. 2010 ¶ 96).

Patent Owner has not provided any other 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 entirety of the trial record and all evidence submitted for claims 1–4, 6, 7, 9, 11–14, 16, 17, and 19. Based on the complete record, we determine that Petitioner has established by a preponderance of the evidence 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 with Suzuki in regards to the “content encryption key” and “content encryption key identifiers” limitations. *See* PO Resp. 40–42. Patent Owner argues that an ordinary artisan could not have been motivated to modify Peterka to better manage multiple content keys obtained multiple segments in advance. *Id.* (citing Ex. 2010 ¶ 96). Patent Owner has not provided any other separate arguments regarding the combined teachings of Peterka, 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 entirety of the trial record and all evidence submitted for claims 5 and 15. Based on the complete record, we determine that Petitioner has established by a preponderance of the evidence that

Peterka in combination with Bocharov, Peterka308, and Chen teaches or suggests the limitations as recited in independent claims 5 and 15.

IV. REVISED MOTION TO AMEND

Because we conclude that all of the challenged claims are unpatentable, we consider Patent Owner's Revised Contingent Motion to Amend. *See* RMTA 1 (stating that "[i]n the event the Board finds the challenged claims unpatentable, Ericsson respectfully requests that the Board grant this revised motion to amend with respect to the corresponding substitute claims").

"Before considering the patentability of any substitute claims, . . . the Board first must determine whether the motion to amend meets the statutory and regulatory requirements set forth in 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121." *Lectrosonics*, Paper 15 at 4 (PTAB Feb. 25, 2019) (precedential). Accordingly, a patent owner must provide a claim listing reproducing each proposed substitute claim, and must make an initial showing to demonstrate the following: (1) the amendment proposes a reasonable number of substitute claims; (2) the proposed claims are supported in the original disclosure (and any earlier filed disclosure for which the benefit of the earlier filing date is sought); (3) the amendment responds to a ground of unpatentability involved in the trial; and (4) the amendment does not seek to enlarge the scope of the claims of the patent or introduce new subject matter. *See* 35 U.S.C. § 326(d); 37 C.F.R. § 42.121.

If the *Lectrosonics* requirements are met, the Board also must assess the patentability of proposed substitute claims "without placing the burden of persuasion on the patent owner." *Aqua Prods.*, 872 F.3d at 1328; *see Lectrosonics*, Paper 15 at 3–4 (discussing *Aqua Products* and the burden of

persuasion). After *Aqua Products*, the Federal Circuit further clarified the burden of persuasion in *Bosch Automotive Service Solutions, LLC v. Matal*, 878 F.3d 1027 (Fed. Cir. 2017), *amended by Bosch Automotive Service Solutions, LLC v. Iancu*, No. 2015-1928 (Fed. Cir. Mar. 15, 2018).

According to *Aqua Products*, *Bosch*, and *Lectrosonics*, a patent owner does not bear the burden of persuasion to show that the proposed substitute claims are patentable. Rather, ordinarily “the petitioner bears the burden of proving that the proposed amended claims are unpatentable by a preponderance of the evidence.” *Bosch*, 878 F.3d at 1040 (as amended on rehearing); *Lectrosonics*, Paper 15 at 3–4. To determine whether a petitioner has proven the substitute claims are unpatentable, the Board focuses on “arguments and theories raised by the petitioner in its petition or opposition to the motion to amend.” *Nike, Inc. v. Adidas AG*, 955 F.3d 45, 51 (Fed. Cir. 2020). The Board itself also may justify any finding of unpatentability by referring to evidence of record in the proceeding. *Lectrosonics*, Paper 15 at 4 (citing *Aqua Products*, 872 F.3d at 1311 (O’Malley, J.)).

A. Proposed Substitute Claims

Patent Owner proposes a set of substitute claims 21–36 in one-to-one correspondence with the set of original claims 1–7, 9, 11–17, and 19 RMTA Claims App’x. Of the proposed substitute claims, claims 21 and 29 are independent. *Id.*

Proposed substitute claim 21 is illustrative, and is reproduced below with underlining to indicate text added to original claim 1 and strike-outs to indicate text removed from original claim 1.

[21.1P] A method for handling secure distribution of content
for over-the-top media delivery comprising:

[21.1] sending a request for live media playback,

- [21.2] receiving a live media playback request response, the live media playback request response comprising content encryption keys and content encryption key identifiers each assigned to an associated content encryption key;
- [21.3] receiving encrypted live media content and manifest files from a content delivery server, 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 and wherein said content encryption key identifiers each uniquely identify each associated content encryption key from every other content encryption key for the entire duration of the encrypted live media content;
- [21.4] applying a first content encryption key to the encrypted live media content before a first time-based content encryption key rotation boundary, the first content encryption key having a first expiration time;
- [21.5] prior to reaching the first time-based content encryption key rotation boundary, and in response to receiving a notification to expire said first content encryption key after a notification-based content encryption key boundary and before said first time-based content encryption key rotation boundary, requesting and obtaining a second content encryption key, the second content encryption key to be used after the notification-based content encryption key boundary and before the first time-based content encryption key rotation boundary is reached; and
- [21.6] applying the second content encryption key for content decryption after the notification-based content encryption key boundary for the first key and before the first time-based content encryption key rotation boundary is reached.

RM TA Claims App'x i–ii (bracketed numbering provided by Patent Owner).

Patent Owner submits that, given that there only one substitute claim per original claim, its proposal is reasonable. RM TA 7 (citing 37 C.F.R. § 42.121(a)(3)). Petitioner does not address this factor. *See generally* Opp. RM TA. We agree with Patent Owner that because there is only one proposed substitute claim per original challenged claim, Patent Owner proposes a reasonable number of substitute claims. *Lectrosonics*, IPR2018-01129, Paper 33 at 45.

B. *Responsiveness to a Ground of Unpatentability Involved in the Trial*

Patent Owner submits that the proposed substitute claims are responsive to the invalidity grounds raised by Petitioner in both the Petition and the opposition to the original motion to amend. RM TA 5–7. In particular, Patent Owner argues that the proposed substitute claims address the issues of uniquely identifying content encryption keys, detection of time-based and notification-based content encryption key rotation boundaries, and requesting and applying keys. *Id.*

Petitioner does not address this factor. *See generally* Opp. RM TA. We agree that Patent Owner has made a sufficient showing that the proposed amendments are responsive to grounds of unpatentability involved in the trial. 37 C.F.R. § 42.121(a)(2)(i).

C. *Scope of Proposed Substitute Claims*

A motion to amend may not enlarge the scope of the claims of the patent. 35 U.S.C. § 316(d)(3); 37 C.F.R. § 42.121(a)(2)(ii). Patent Owner contends the proposed substitute claims do not enlarge the scope of the original claims because they “retain all features of the corresponding original claims, and only add clarifying or narrowing limitations.” RM TA 1.

In particular, Patent Owner argues that the claims “now explicitly require that the second content encryption key be applied *after* the notification-based content encryption key rotation boundary and *before* the time-based rotation boundary.” *Id.* at 2.

Petitioner argues, however, that the proposed substitute claims broaden the scope of the challenged claims. Opp. RMTA 2–5. In particular, Petitioner points out that, for example, original claim 1:

[R]ecited a first “key rotation boundary” (hereafter, “*Boundary*”) and required two actions relative to that claimed *Boundary*: (1) “*prior to* reaching the [*Boundary*], obtaining a second [CEK]” and (2) “applying the second [CEK] for content decryption *after* the [same *Boundary*] is reached.”

Opp. RMTA 2 (citing Ex. 1001, claim 1). Petitioner refers to this requirement as an “‘prior to/after’ sequence.” *Id.* at 3. Petitioner further argues that proposed claim 21, that would substitute for claim 1, recites “separate boundaries: a “‘*notification-based*’ boundary and a ‘*time-based*’ boundary.” *Id.* Petitioner focuses on two of the new claim 21 requirements that include these boundaries:

[21.5]/[29.6] *prior to* reaching the first time-based [CEK] rotation boundary, and in response to receiving a notification to expire said first [CEK] after a notification-based [CEK] boundary and before said first time-based [CEK] rotation boundary, request[ing] and obtain[ing] a second [CEK], the second [CEK] to be used *after* the notification based [CEK] boundary and before the first time-based [CEK] boundary is reached; and

[21.6]/[29.7] apply[ing] the second [CEK] for content decryption *after* the notification-based [CEK] boundary for the first key and before the first time-based [CEK] rotation boundary is reached.

Opp. RMTA 3 (citing RMTA Claims App’x, ii, iv-v) (emphasis supplied by Petitioner). Petitioner argues that claim 21 “do[es] not preserve the same sequence of (1) obtaining a second CEK *prior to a Boundary and* (2) applying a second CEK *after that same Boundary*. *Id.* According to Petitioner, the request to retrieve the second CEK is made “in response to” a notification-based CEK boundary, rather than made ahead of that boundary. *Id.* Thus, for the notification-based boundary, the substitute claims are not limited to the “prior to/after” sequence, but also cover an “after/after” sequence — and thus improperly broaden the claims. *Id.* at 3–4. Alternatively, for the time-based boundary, again the request to retrieve the second key is not fixed in relation to the boundary, but in any event the key must be applied before the boundary. Again, argues Petitioner, the “prior to/after” sequence is not preserved, and the claims are too broad. *Id.* at 4.

Patent Owner argues that the substitute claims do not broaden the original claims, because the requirement that the second CEK is “in response to” a notification of an upcoming notification-based boundary, and that necessarily means that second key is obtained before the notification-based boundary and applied after that boundary. Reply RMTA 3. Patent Owner also argues that the timing of obtaining and applying the second key in relation to the time-based boundary is not relevant, because the proper focus is on the actual boundary that defines the point of key rotation. *Id.*

Petitioner replies that there is no basis for Patent Owner’s assumption that the claims require the second key to be requested and obtained “in response to” a “notification” of an “upcoming” notification-based boundary. Sur-Reply RMTA 2. Instead, argues Petitioner, the notification of the boundary can occur at the time the boundary occurs, or even afterwards, given that the ’313 patent describes notifications of boundaries that are not

“upcoming.” *Id.* (citing Ex. 1001, 4:22–24, 7:33–37, 7:67–8:10, 9:20–22, 10:60–11:8, 11:24–34.).

Furthermore, argues Petitioner, even if the notification of the boundary occurs before the boundary, the request for/obtaining of a second CEK “in respond” to the “notification to change key” does not have to occur before the boundary, due to a delay in the response. Sur-Reply RMTA 5–6.

We agree with Petitioner that the substitute claims are broadening. Because the amended wording only requires obtaining the second key CEK “in response to detecting” the boundary, rather than “prior to” the boundary, the second CEK can be obtained before or after the boundary. This is not a fanciful or unlikely possibility — such delayed requests are specifically contemplated by the ’313 patent:

[I]f the packager 104 is unable to obtain a new content encryption key from the WFM 102 prior to the expiration of the current content encryption key, the packager 104 will continue to use the current content encryption key until such time as it is able to obtain a new key from the WFM 102.

Ex. 1001, 6:43–48.

It should be noted that the fixed period duration for key rotation may be viewed as a “target” period, as the packager 104 may not expire a key on the exact boundary.

Ex. 1001, 8:23–25.

The key expiration time from the WFM 102 may be viewed as a “suggested” expiration time, as the packager 104 may not be able to expire the key at the exact specified time.

Ex. 1001, 9:16–19.

If the new content encryption key has not been retrieved yet (e.g., due to . . . content encryption key retrieval failures . . .)

Ex. 1001, 11:37–44.

Therefore, based on our review of the record we conclude that Patent Owner has failed to make a sufficient showing that the proposed substitute claims do not enlarge the scope of the claims.

D. *Support for Proposed Substitute Claims*

New subject matter is any addition to the claims that lacks sufficient support in the subject patent’s original disclosure. *See TurboCare Div. of Demag Delaval Turbomach v. Gen. Elec. Co.*, 264 F.3d 1111, 1118 (Fed. Cir. 2001) (“When [an] applicant adds a claim . . . , the new claim[] must . . . find support in the original specification.”). The Board requires that a patent owner show in a motion to amend that there is written-description support in the originally filed disclosure of the subject patent for each proposed substitute claim, and also set forth support in an earlier-filed disclosure for each claim for which the patent owner seeks the benefit of the earlier-filed disclosure’s filing date. *See* 37 C.F.R. §§ 42.121(b)(1), 42.121(b)(2).

To support its contention that the proposed substitute claims have sufficient support, Patent Owner provides a chart that identifies support for the proposed substitute claims in the ’313 Patent. RMTA 7–13. Patent Owner submits that a “each substitute claim is supported by each earlier-filed disclosure as to which the benefit of the filing date is sought.” *Id.* at 7–8 (citing ’313 Patent Application Publ. No. 2020/0068241 (“the ’313 Publication,” Ex. 2004); U.S. provisional app. 61/500,316 (“the Provisional Application,” Ex. 2005); U.S. Patent Application Publ. No. 2018/0192102 (Ex. 2006)); U.S. Patent Application Publ. No. 2016/0198203 (Ex. 2007); U.S. Pat. No. 9,313,178 (Apr. 12, 2016) (Ex. 2008); and U.S. Pat. No. 8,751,807 (Jun. 10, 2014) (Ex. 2009). In particular, Patent Owner addresses claim support issues raised by Petitioner in its opposition to the original motion to amend (Paper 27), and discussed in our Preliminary Guidance

(Paper 31), regarding the “content encryption key identifiers,” “issuing requests to . . . retrieve a second content encryption key,” and “applying the second key” claim requirements. *Id.* at 8–10.

Petitioner in opposition renews its contention that the original disclosure still does not support the “applying the second CEK” claim requirements in their current form — specifically, the substitute claim 21.6 requirement, “apply[ing] the second [CEK] for content decryption after the notification-based [CEK] boundary for the first key and *before* the first time-based [CEK] rotation boundary is reached,” and the commensurate requirement of substitute claim 29. Opp. RMTA 5–7.

Petitioner argues that “no original claim required that a second key be applied for decryption *before* the demarcating rotation boundary,” and that likewise none of the other portions of the ’313 Publication on which Patent Owner relies (Ex. 2004, Fig. 3, ¶¶ 6, 35–37, claims 1, 16) support the requirement of “applying the second key for content decryption . . . before said time-based content encryption key rotation boundary for said first key is reached.” Opp. RMTA 6. Petitioner argues that it would not make sense to require the second key to be applied before the time-based content encryption key rotation boundary for the first key is reached, because:

In the “normal period-based expiration” case, the second key is applied for decryption *after* a rotation boundary. In the “explicit key change notification” case, replacement keys are applied independent of and, agnostic to, key rotation boundaries.

RMTA 7.

In reply, Patent Owner asserts that the Provisional Application discloses content encryption keys that initially come with a content key expiration point, and that subsequently there is a check for an unscheduled

key change outside of the fixed duration lifespan. Reply RMTA 6 (citing Ex. 2005, Fig. 3 (steps 304, 308), pp. 11–12).¹² Patent Owner further argues that this discloses that a key change notification can alter the original point of key rotation, and therefore explicit key change notifications are *not* “independent of and, agnostic to, key rotation boundaries,” as Petitioner argues. *Id.* (citing Opp. RMTA 7).

In addition, Patent Owner cites disclosures that unscheduled key rotations can occur “at *any* time,” that unscheduled security-related key changes necessarily occur before the original time-based key rotation point, and that a key may be expired before its fixed duration lifespan — for example, with “10 minutes left in its lifespan.” Reply RMTA 6–7 (citing Ex. 2005, pp. 5, 8–10).

Petitioner objects to Patent Owner’s reliance in portions of the Provisional Application that were not relied on until the Reply. Sur-Reply RMTA 7. Also, Petitioner argues that Patent Owner’s reliance on the disclosure that unscheduled key rotations can occur “at any time” actually supports Petitioner’s argument that replacement keys are applied independent of (and agnostic to) existing key rotation boundaries. *Id.* at 8. Likewise, argues Petitioner, the disclosures of determining expiration times for unscheduled keys does not support a requirement that a replacement key be applied before a time-based content encryption key rotation boundary. *Id.*

We agree with Patent Owner that the revised amended claims are supported. As we advised in the Preliminary Guidance:

¹² Patent Owner asserts that the other priority documents (Exhibits 2006, 2007, and 2008) have the same disclosures as the Provisional Application. Reply RMTA 7.

The '241 publication describes circumstances in which “a key change is signaled . . . outside of any fixed duration lifespan” for security reasons (Ex. 2004 ¶ 36) such that the current content encryption key is expired early and “the client [] must issue a new content encryption key request to the license server [] to retrieve the new content encryption key, then replace the current content encryption key with the newly retrieved content encryption key” (*id.* ¶ 37).

Paper 29 at 9–10. Although the original amended claims did not provide support for the full scope of the then-existing substitute claim limitation because the claim limitation allowed for the second key for content decryption to be applied before or after the notification-based content encryption key rotation boundary, the revised substitute claims have addressed that issue.

E. Alleged Obviousness of Claims 21–24, 26, 27, and 29–32 over Peterka and Traw

Petitioner challenges substitute claims 21–24, 26, 27, and 29–32 as obvious over Peterka and Traw. Opp. RMTA 7–23.

1. Traw

Traw, titled “Proactive Forced Renewal Of Content Protection Implementations,” was filed April 13, 2004, and issues as US 7,392,381 B2 on June 24, 2008. Ex. 1042, codes (54), (22), (10), (45). Traw is directed to:

A system for proactive forced renewal of content protection implementations in devices includes a key generation facility to generate and allocate keys for the devices, and to generate revocation data corresponding to revoked keys in response to at least one of a security compromise and on a periodic basis independent of a security compromise

Ex. 1042, code (57), *see* 1:65–2:6. The Traw system is applicable “for protecting content (such as audiovisual entertainment content) against unauthorized access, copying or distribution. *Id.* at 2:15–19. The systems

include provisions for proactively revoking encryption keys on a periodic basis, such as providing keys with expiration times. *Id.* at 3:4–6, 3:62–66, 5:14–17, 5:33–35, 6:10–12. The system also can generate a non-scheduled revocation of a key if it determines that it should be revoked if it has been compromised. *Id.* at 4:37–39, 6:39–44.

2. *The Combination of Peterka and Traw*

Petitioner contends a person of ordinary skill in the art would have been motivated to combine Peterka and Traw because (1) the references are in the same field of art (Opp. RMTA 9–10 (citing Ex. 1005, Figs. 7B, 8, 14, ¶¶ 80, 82, 105–106, 110, 116–121, 130; Ex. 1042, Abs., Figs. 1–3, 1:65–2:2, 2:56–60, 3:13–19, 3:32–46, 3:63–66, 4:11–14, 5:5–19); Ex. 1041 ¶¶ 263–264); (2) the references “share common objectives to prevent unauthorized access to content” (*id.* at 10 (citing Ex. 1005 ¶¶ 105, 110, 121, 135–146; Ex. 1042, 2:15–19, 3:63–66); Ex. 1041 ¶¶ 265–266); and (3) persons of ordinary skill in the art would have understood “that notwithstanding Peterka’s described security mechanisms including key rotation, the security of systems like Peterka’s could be improved to address breaches” (*id.* at 10–11 (citing Ex. 1005 ¶ 110; Ex. 1042, 6:39–57; Ex. 1040, 135:20–136:25, 139:7–140:24; Ex. 1041 ¶¶ 266–267)).

Petitioner argues that a person of ordinary skill in the art would have been motivated to improve Peterka’s system (*see* EX1040, 135:20–136:5, 139:7–140:24; *see also id.*, 136:6–25) in view of Traw by: (1) providing a notification to clients that a certain key is compromised and requires early expiration (Traw, 5:63–65, 4:62–65) using Peterka’s content packet “signaling methods” for key changes (Pet., 11; Peterka, [0116]–[0120]); (2) having the client obtain a replacement key using Peterka’s “pull” method (Pet., 11–12; Peterka, [0105]–[0106]) when notified that the current key has been revoked before the originally-scheduled expiration of the compromised key (Traw,

6:18–21); and (3) having the client apply the replacement key for decryption when the replacement key is received, before the originally-scheduled expiration of the compromised key in order to minimize service interruptions (Peterka, [0105]). EX1041, ¶268.

Opp. RMTA 11–12. Petitioner also contends persons of ordinary skill in the art would have had a reasonable expectation of success in combining Peterka and Traw “because Traw teaches a straightforward way to address security breaches easily adaptable to Peterka.” *Id.* at 12 (citing Ex. 1005 ¶¶ 105–106, 116–121, 135–138; Ex. 1041 ¶ 269).

Patent Owner does not specifically address the issue of motivation to combine Peterka and Traw. *See generally* RMTA; Reply RMTA; Sur-Reply RMTA 8. Nonetheless the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. We find, based on the entire record, that Petitioner has proven by a preponderance of the evidence that a person of ordinary skill in the art would have been motivated to combine the teachings of Peterka with Traw as proffered by Petitioner with a reasonable expectation of success.

3. *Substitute Claims 21 and 29*

Petitioner contends Peterka teaches proposed substitute claim limitations [21.P], [21.1], and [21.3] for the reasons set forth in its challenge in the Petition of claim 1 as obvious over Peterka. Opp. RMTA 12 (citing Pet. 3, 19–22, 28–31, 57; Ex. 1003 ¶ 178; Ex. 1005, Fig. 1, ¶¶ 15, 38; Ex. 1047 ¶¶ 344–345, 358). For substitute claim 29, Petitioner relies on its arguments for original claim 11 and substitute claim 21. *Id.* at 23 (citing Ex. 1047 ¶ 350).

We address amended limitations [21.2], [21.3], [21.4], [21.5], and [21.6] below.

a) *Limitations [21.2] and [21.3]*

Petitioner contends Peterka teaches content encryption key identifiers requirements of claim limitation [21.2] by describing assigning a sequence number or timestamp to a client along with an associated content encryption key in an Entitlement Management Message (EMM) or Entitlement Control Message (ECM). Opp. RMTA 13–15. Petitioner contends a person of ordinary skill in the art would have understood that the sequence number or timestamp constitutes a unique encryption code identifier that identifies the specific key in the ECM/EMM message. *Id.* at 13 (citing Pet. 25–26; Ex. 1005 ¶ 121; Ex. 1003 ¶¶ 91–92; Ex. 1041 ¶ 239). Petitioner points out that the encryption key identifiers in the ’313 patent include data such as “a segment number of the prepared content,” which is analogous to the sequence number or timestamp of the Peterka messages. Opp. RMTA (citing Ex. 1001, 3:43–45, 4:17–18, 6:12–16, 6:28–30.; Ex. 1047 ¶¶ 304–307); Sur-Reply RMTA 8–9.

Alternatively, Petitioner argues that “directly ‘assign[ing]’ an identifier ‘to an associated [CEK]’ would have been obvious,” motivated by the use of unique key identifiers CK₀, CK₁, and CK₂ in Figure 7B of Peterka, and the use of “key IDs” disclosed in Traw, as well as the fact that use of unique key identifiers was a well-known technique. Opp. RMTA 13–14 (citing Pet. 25; Ex. 1042, 3:32–46, 4:45; Ex. 1003 ¶¶ 91–94; Ex. 1047 ¶¶ 304–307); Sur-Reply RMTA 9.

In addition, for claim limitation [21.3], Petitioner contends a person of ordinary skill in the art would have understood that, because each sequence number or timestamp is specifically included “*to protect against replay attacks*” during media playback,” each sequence number/timestamp “‘uniquely identif[ies] each’ ECM/EMM (and ‘[CEK]’ within) ‘from every

other’ ECM/EMM and corresponding ‘[CEK] for the entire duration of a media playback.’” Opp. RMTA 15 (citing Ex. 1005 ¶ 121; Ex. 1047 ¶¶ 311–312).

Petitioner also argues that, in the alternative, ensuring uniqueness of key identifiers “for the entire duration of the media playback” was obvious, as illustrated by Peterka’s Figure 7B, showing content key identifiers, CK₀, CK₁, and CK₂, that are unique for the entire program’s duration. Opp. RMTA 15–16 (citing Ex. 1005, Figs. 7A, 7B, ¶ 92; Ex. 1003 ¶¶ 92–94; Ex. 1047 ¶¶ 314–315).

In reply, Patent Owner substantially repeats its arguments against Petitioner’s reliance on Peterka for the claim 1 content encryption key identifiers requirements. Reply RMTA 8–9 (citing Ex. 1005 ¶ 121; Ex. 2010 ¶¶ 88, 93–94); *see* RMTA 14–15. We are not persuaded by these arguments for the reasons discussed above.

b) Limitation [21.4]

For the “first key having a first expiration time” requirement of claim 21, Petitioner relies on the disclosure in Peterka of encryption keys that are periodically rotated in accord with an associated “time remaining in the lifetime of the key.” Opp. RMTA 16 (citing Ex. 1005, Fig. 8, ¶¶ 82, 90, 92, 105–106, 108, 110, 116, 121; Ex. 1003 ¶ 51, 121; Ex. 1047 ¶¶ 316, 318).

c) Limitation [21.5]

For the “notification” requirement of claim 21, Petitioner relies on the disclosure in Traw of revoking a time-based key that has been compromised due to a security breach before that key would ordinarily be rotated, and notifying client devices of such revocations using the key change signaling methods of Peterka. Opp. RMTA 16–19 (citing Ex. 1005

¶¶ 105, 110, 116–121; Ex. 1042, 3:17–19, 4:62–65, 5:29–31, 5:35–39, 5:63–65, 6:12–21, 6:39–57; Ex. 1047 ¶¶ 323–330).

d) Limitation [21.6]

For the “applying the second content encryption key . . . after the notification-based CEK boundary” requirement of claim 21, Petitioner relies on the disclosures in Peterka that the client keeps track of its keys under the pull method and issues a request for a new key to avoid service interruptions, and argues that a person of ordinary skill would have been motivated to implement the Peterka/Traw combination such that a client would request a new key immediately, so that it would be used before the current (compromised) key was set to expire. Opp. RMTA 17–19 (citing Ex. 1005 ¶¶ 105–106, 116; Ex. 1042, 2:43–64, 3:17–19, 4:63–65, 5:35–65, 6:12–21, 6:39–57; Ex. 1047 ¶¶ 331–332).

In reply, Patent Owner argues that Petitioner does not identify any teaching in Peterka or Traw of content encryption key identifiers but rather only provides message identifiers. Reply RMTA 8; *see* RMTA 16–17. Patent Owner further argues that because Peterka’s message identifiers already serve to uniquely identify keys and to avoid key confusion, there would be no reason for an ordinarily skilled artisan to modify Peterka and add content encryption key identifiers. Reply RMTA 9. Patent Owner then repeats its argument that the signaling described in Peterka only alerts clients about keys that have already been provided, rather than receiving a key change notification in response to a key rotation boundary notification. *Id.* at 10 (citing Ex. 1005 ¶¶ 116–117; Ex. 2010 ¶¶ 120–129). Patent Owner also submits that Traw also teaches that a notification instructs the client to change to a key that the client has already been provided. *Id.* at 10–11 (citing Ex. 1041, Abstr., 2:43–64, 5:7–65; Ex. 2010 ¶¶ 94–95).

Petitioner responds that the combination of Peterka and Traw teaches or suggests this limitation, that Peterka’s pull method is not limited to requesting keys that have already been provided, and that Traw “discloses ‘requir[ing]’ content protection implementations to be ‘renewable . . . *in the event* of revocation’ (e.g., in response to a revocation due to a compromised key), which Traw says can be through downloading ‘a new content protection implementation.’” Sur-Reply RMTA 9–11 (citing Ex. 1005 ¶¶ 106, 110; Ex. 1041, 2:43–64, 5:8–12, 5:27–33, cl. 1; Ex. 1047 ¶¶ 327–330). Petitioner also argues that Patent Owner fails to refute that a person of ordinary skill:

would have been motivated to implement Peterka-Traw to minimize “service interruptions” (Peterka, [0105]), such that when the client receives the second key due to an unscheduled key revocation (Traw, 3:17-19, 4:63-65, 5:35-39, 5:63-65, 6:12-21, 6:39-57), the client promptly applies the second key for decryption, before the current key is set to expire, allowing the client to resume viewing content.

Id. at 11 (citing Ex. 1005 ¶¶ 106, 116; Ex. 1003 ¶ 115; Ex. 1047 ¶ 332).

We are not persuaded by Patent Owner’s arguments and agree with Petitioner regarding Limitation 21.5.

e) Claims 21 and 29 Summary

Other than Patent Owner’s arguments directed to specific limitations discussed above, which we do not find persuasive, Patent Owner does not otherwise specifically respond to any of Petitioner’s other arguments regarding substitute claims 21 and 29 as obvious over Peterka and Traw. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. Accordingly, having considered and weighed the entirety of the evidence,

we determine that Petitioner has proved by a preponderance of the evidence that substitute claims 21 and 29 would be unpatentable under 35 U.S.C. § 103(a) over the combination of Peterka and Traw.

4. *Substitute Claims 22, 23, 27, 30, and 31*¹³

Substitute claims 22, 23, 27, 30, and 31, add requirements that a second content encryption key that is replacing the previous key have an expiration time that is set to equal the remaining lifespan of the previous key when it was expired. Petitioner argues that this expiration time option was obvious to try based on practical considerations such as accommodating already-staged key rotation boundaries tied to future media segments and handling potential latency issues. Opp. RMTA 20–23 (citing Pet. 34–41; Ex. 1005, Fig. 7B, ¶¶ 80, 122; Ex. 1041, 3:35, 4:45; Ex. 1047 ¶¶ 335–349).

Patent Owner disagrees with Petitioner’s argument that the expiration time requirement would have been obvious to try is unsound because it relies on an open-ended selection or possible choices. RMTA 20–23; Reply RMTA 11–12. We agree with Petitioner, however that a person of ordinary skill:

would have specifically been motivated to set the expiration time for the second (replacement) CEK *after* the expiration of the first (compromised) key, such that “the second CEK’s expiration time” is “equal to the remaining lifespan for the pre-existing expiration set for the first CEK plus the fixed expiration time (period duration) originally assigned for the first CEK.”

Sur-Reply RMTA 12 (citing Ex. 1047 ¶¶ 343–344).

¹³ For substitute claims 24, 26, 29–32, and 35, Petitioner relies on its challenges of claims 4–6 and 11 as obvious over Peterka. Opp. RMTA 22–23 (citing Pet. 38–42; Ex. 1047 ¶¶ 345, 350).

Substitute claims 27 and 37 add requirements that the second content encryption key is applied to decrypt the same content segment for which the first content encryption key was used, and the notification-based expiration of the first content encryption key is for security reasons. Petitioner relies on the modified system in Peterka/Traw that includes a mechanism for responding to security attacks: revoking and requiring replacement of a compromised key before its set expiration. Opp. RMTA 23 (citing Pet. 10, 36–37; Ex. 1005, Figs. 7A, 7B, ¶¶ 80–82, 91–101, 106, 116, 121–125; Ex. 1041, Fig. 2, 1:65–2:2, 2:15–19, 3:65–66, 4:37–39, 5:5–39; Ex. 1047 ¶¶ 348–349).

Patent Owner argues, for claim 27, that Peterka teaches that each key is for one segment, and there is only one segment per key, and that Traw does not teach using the second key to decrypt the same content segment as the first key. RMTA 21–22 (citing Ex. 1003 ¶ 76); Reply RMTA 12. We agree with Petitioner, however, that Patent Owner attacks the individual teachings of Peterka and Traw, while Petitioner relies on the teachings of the combination that a compromised key is revoked and replaced before its set expiration. Sur-Reply RMTA 12 (citing Ex. 1047 ¶¶ 348–349).

Based on the above analysis, having considered and weighed the entirety of the evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 22–24, 26, 27, 29–32, and 35 are unpatentable under 35 U.S.C. § 103(a) over the combination of Peterka and Traw.

F. Alleged Obviousness of Claims 21–36

Petitioner also contends persons of ordinary skill in the art would “have combined Traw with the original grounds set forth in the Petition, for the same reasons” discussed above (Opp. RMTA 24 (citing *id.* § II.A.3;

Ex. 1047 ¶ 351)), and argues that those combinations “meet substitute claims 21–24, 26–27, 29–32, and 35 for the same reasons discussed *supra* §§II.A.4–II.A.9, *and also* meet substitute claims 25, 28, and 33 for the reasons discussed in Grounds 2–5” (*id.*).

Petitioner specifically argues that Suzuki’s key number teachings render obvious the content encryption key identifiers requirements of claim limitation [21.2]. Opp.RMTA 24–25 (citing Pet. 46–50, 60–63; Ex. 1005, Figs. 7A, 7B, ¶ 92; Ex. 1006, Fig. 2, ¶¶ 13, 30, 43–48, 80; Ex. 1003 ¶¶ 153, 186–192; Ex. 1047 ¶¶ 353–354).

Patent Owner generally relies on its arguments for Ground 6A, which we find unpersuasive. Accordingly, based on the above analysis, having considered and weighed the entirety of the evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 21–36 are unpatentable under 35 U.S.C. § 103(a) over the combinations asserted by Petitioner in Grounds 6B–6E.

G. Summary

Because we have determined that Patent Owner has not demonstrated that the motion to amend meets the statutory and regulatory requirements set forth in 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121, and Petitioner has proved by a preponderance of the evidence that the substitute claims are unpatentable under 35 U.S.C. § 103(a), we deny Patent Owner’s revised motion to amend.

V. CONCLUSION

For the foregoing reasons, we are persuaded that Petitioner establishes by a preponderance of the evidence that claims 1–7, 9, 11–17, and 19 of the '313 patent have been shown to be unpatentable.

In summary:

Claims	35 U.S.C. §	References/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–4, 6, 7, 11–14, 16, 17	103	Peterka	1–4, 6, 7, 11–14, 16, 17	
1–4, 6, 7, 11–14, 16, 17	103	Peterka, Suzuki	1–4, 6, 7, 11–14, 16, 17	
1–4, 6, 7, 9, 11–14, 16, 17, 19	103	Peterka, Bocharov	1–4, 6, 7, 9, 11–14, 16, 17, 19	
1–4, 6, 7, 9, 11–14, 16, 17, 19	103	Peterka, Suzuki, Bocharov	1–4, 6, 7, 9, 11–14, 16, 17, 19	
5, 15	103	Peterka, Bocharov, Peterka308, Chen	5, 15	
Overall Outcome			1–7, 9, 11–17, 19	

The table below summarizes our conclusions as to Patent Owner's Revised Motion to Amend the claims.

Motion to Amend Outcome	Claims
Original Claims Canceled by Amendment	1–7, 9, 11–17, 19
Substitute Claims Proposed in the Amendment	21–36
Substitute Claims: Motion to Amend Granted	
Substitute Claims: Motion to Amend Denied	21–36
Substitute Claims: Not Reached	

VI. ORDER

In consideration of the foregoing, it is hereby
ORDERED that claims 1–7, 9, 11–17, and 19 of U.S. Patent
No. 11,122,313 B2 have been shown to be unpatentable under 35 U.S.C.
§ 103;

FURTHER ORDERED that Patent Owner's Revised Motion to
Amend (Paper 31) is *denied*; and

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

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 Knops
NOROOZI PC
peter@noroozipc.com

Exhibit B

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE OFFICE OF THE UNDER SECRETARY OF COMMERCE
FOR INTELLECTUAL PROPERTY AND DIRECTOR OF THE
UNITED STATES PATENT AND TRADEMARK OFFICE

GOOGLE LLC,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

IPR2025-00003 (Patent 9,313,178 B2)
IPR2025-00004 (Patent 11,122,313 B2)¹

Before JOHN A. SQUIRES, *Under Secretary of Commerce for Intellectual
Property and Director of the United States Patent and Trademark Office.*

ORDER

¹ This order applies to each of the above-listed proceedings.

IPR2025-00003 (Patent 9,313,178 B2)
IPR2025-00004 (Patent 11,122,313 B2)

The Office received a request for Director Review of the Final Written Decision in each of the above-captioned cases and an authorized response to each request. *See* Papers 44, 45.²

Having considered the requests and responses, it is:

ORDERED that the requests for Director Review are denied.

² Citations are to the record in IPR2025-00003. The parties filed similar papers in IPR2025-00004.

IPR2025-00003 (Patent 9,313,178 B2)
IPR2025-00004 (Patent 11,122,313 B2)

FOR PETITIONER:

Scott A. McKeown
Anant K. Saraswat
WOLF, GREENFIELD & SACKS, P.C.
smckeown-ptab@wolfgreenfield.com
asaraswat-ptab@wolfgreenfield.com

PATENT OWNER:

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