

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

ERICSSON AB,
Patent Owner.

IPR2025-00003
Patent 9,313,178 B2

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

BEAMER, *Administrative Patent Judge*.

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

I. INTRODUCTION

Google LLC (“Petitioner”) filed a Petition (“Pet.”) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–8, 10, 12, 14, and 16–20 of U.S. Patent No. 9,313,178 B2 (“the ’178 patent”).¹ Paper 3. We instituted *inter partes* review of all the claims challenged in the Petition. Paper 14 (“Inst. Dec.”). Ericsson AB (“Patent Owner”) filed a Patent Owner Response to the Petition. Paper 25 (“PO Resp.”). Petitioner filed a Reply and Patent Owner filed a Sur-Reply. Paper 31 (“Reply”); Paper 34 (“Sur-Reply”). Patent Owner also filed a Motion to Amend the claims, Petitioner filed an Opposition to that Motion, and we provided Preliminary Guidance under the Board’s Motion to Amend Pilot Program. Papers 24, 28, 30.

Thereafter, Patent Owner filed a Revised Motion to Amend, Petitioner filed an Opposition, Patent Owner filed a Reply, and Petitioner filed a Sur-Reply. Paper 32 (“RMTA”); Paper 35 (“Opp. RMTA”); Paper 38 (“Reply RMTA”); Paper 40 (“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, and a copy of the transcript was entered into the record. Paper 42 (“Tr.”).

We have jurisdiction over this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). Based on the complete record, we find that Petitioner has shown, by a preponderance of the evidence, that claims 1–8, 10, 12, 14, and 16–20 of

¹ Co-Petitioner Lenovo (United States) Inc. was terminated from this proceeding due to settlement. Paper 20.

the '178 patent are unpatentable. Also, we determine that Patent Owner's Revised Motion to Amend should be denied.

II. BACKGROUND

A. The '178 Patent

The '178 patent, titled "Method And System For Secure Over-The-Top Live Video Delivery," was filed on April 30, 2014, issued on April 12, 2016, and lists a related continuation application filed June 22, 2012, and related provisional application filed June 23, 2011.² Ex. 1001, codes (54), (22), (45), (63), (60).

The '178 patent is directed to managing encryption key rotation (use of a series of encryption keys) and secure key distribution in "over-the-top" content delivery, which is the delivery of media content over the public Internet. Ex. 1001, code (57), 1:15–20. Key rotation is called for when live streaming content with long or indefinite durations, because the use of a single encryption key for the entire duration increases the probability that the key may be compromised. *Id.* at 1:23–26. As an example, MPEG video content is divided into segments of fixed duration, and the segments are encrypted with encryption keys. *Id.* at 2:53–64. Figure 1 is reproduced below.

² The effective priority date for the claims is not at issue here. Pet. 7.

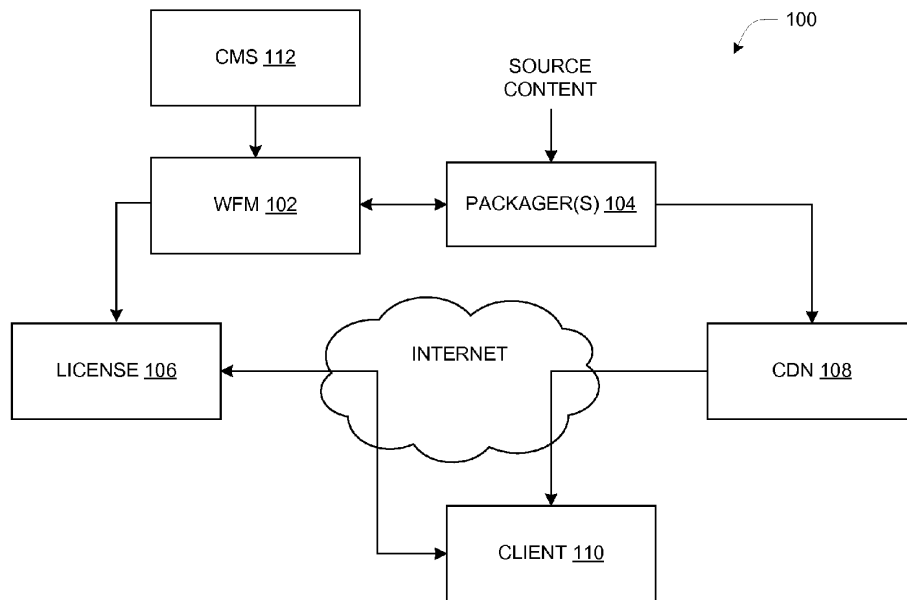


Fig. 1

Figure 1 is a block diagram of a content delivery system. Ex. 1001, 4:39. Content management system (CMS) 112 provides high-level control over content ingestion, packaging and delivery. *Id.* at 5:15–17. Workflow manager (WFM) 102 performs more detailed control operations for preparation of live content, including generation of content encryption keys. *Id.* at 5:17–18, 5:21–25, 6:10–13, 6:29–32. License server 106 is responsible for storing encryption keys and providing them to the client 110 for use during playback. *Id.* at 5:18–20. The license server registers client devices and verifies the right of each client device to view the content. *Id.* at 6:64–67. Packager(s) 104 receive source content from workflow manager (WFM) 102 and process the content for delivery to clients 110 via the content delivery network (CDN) 108. *Id.* at 5:11–13, 6:38–40. The packagers segment output files into fixed duration segments, and perform

content encryption using a series of encryption keys. *Id.* at 5:13–15, 5:40–44, 6:2–7. In one embodiment, when initiating playback, the client requests the current content encryption key and the next future content encryption key. *Id.* at 3:47–50.

In an exemplary embodiment, each encryption key is assigned a unique identifier based, for example, on wall clock time or segment number. *Id.* at 3:29–36. Each key is also assigned a preset expiration time, measured by relative wall clock time, segment numbers, or number of video key frames. *Id.* at 6:13–25. The fixed period duration for key rotation is a “target” or “suggested period,” as the packager may not be able to expire the key at the exact specified time. *Id.* at 8:9–11, 9:1–4.

Also, WFM 102 can push a new content encryption key to packager 104 ahead of time when the current content encryption key is deemed to be no longer secure (*e.g.*, if the content encryption key has been compromised). *Id.* at 7:17–20. Packager 104 waits until the next available encryption boundary (which could be a segment boundary) before applying the new content encryption key. *Id.* at 7:20–25. The client can be notified 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 7:53–56, 10:52–57.

Figure 3 is reproduced below.

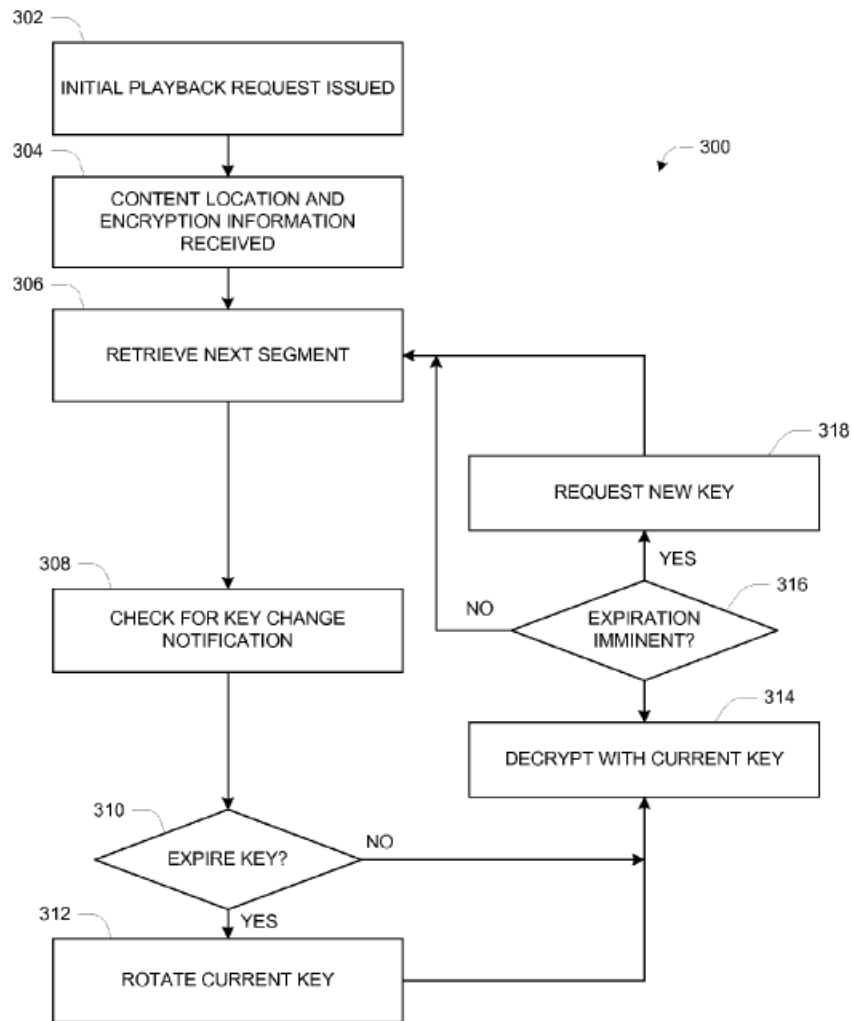


Fig. 3

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, 4:42–43, 9:47–49. 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 9:47–56, 10:25–38, 11:32–37. 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 1:63–65, 11:3–12. 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.³ *Id.* at 11:38–45. However, there can be content encryption key retrieval failures in step 318, 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 11:18–25.

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, 10:40–43, 10:65–11:2. 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.*

B. Illustrative Claim

Independent claim 1 is illustrative of the challenged claims, and follows:

1. A method for handling secure distribution of content comprising:
initiating a media playback request and receiving a
playback request response;

³ 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.

parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;

retrieving content and manifest files from a content delivery server;

detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

issuing requests to a 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

applying the second key for content decryption after the key rotation boundary is reached.

Ex. 1001, 12:2–21; Pet. x.

C. Evidence of Record and Challenges to Patentability

Petitioner challenges the patentability of claims 1–8, 10, 12, 14, and 16–20 of the '178 patent on the following basis (Pet. 7):

Claims Challenged	35 U.S.C. §⁴	References
1–6, 10, 12, 16–18, 20	103	Peterka ⁵
1–6, 10, 12, 16–18, 20	103	Peterka, Suzuki ⁶

⁴ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), included amendments to 35 U.S.C. §§ 102 and 103 effective March 16, 2013, which is after the '178 patent's assumed June 23, 2011 priority date. *See* Pet. 7; Ex. 1001, code (60). Therefore, for purposes here, we apply the pre-AIA version of Section 103.

⁵ Peterka, US 2002/0172368 A1. Ex. 1005 (“Peterka”).

⁶ Suzuki, et al., 2004-166153. Ex. 1006 (“Suzuki”).

Claims Challenged	35 U.S.C. § ⁴	References
1–6, 10, 12, 14, 16–18, 20	103	Peterka, Bocharov ⁷
1–6, 10, 12, 14, 16–18, 20	103	Peterka, Suzuki, Bocharov
7, 8, 19	103	Peterka, Bocharov, Peterka308, ⁸ Chen ⁹

Petitioner filed a Declaration, a Supplemental Declaration, and a Second Supplemental Declaration of Anthony J. Wechselberger in support of the Petition and in opposition to the motions to amend. Exs. 1003, 1041, 1047.

Patent Owner filed a Declaration Of John Villasenor, Ph.D. In Support Of Patent Owner’s Response. Ex. 2010.

D. Real Parties in Interest

Petitioner identifies itself as the real party in interest. Pet. 4. Patent Owner identifies Ericsson AB, Ericsson Inc., and Telefonaktiebolaget LM Ericsson as real parties in interest. Paper 5, 1.

E. Related Proceedings

The parties identify as related matters: *Ericsson Inc. et al. v. Samsung Electronics Co., Ltd. et al.*, No. 2:21-cv-00001; *Telefonaktiebolaget LM Ericsson et al. v. Lenovo (United States), Inc. et al.*, No. 5:23-cv-00570; *Certain Electronic Devices with Wireless Connectivity, Components Thereof, and Products Containing Same*, Inv. No. 337-TA-1245; *Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components*

⁷ Bocharov, et al., US 2010/0235528 A1. Ex. 1007 (“Bocharov”).

⁸ Peterka, et al., US 2008/0270308 A1. Ex. 1008 (“Peterka308”).

⁹ Chen, et al., EP 1 418 756 A2. Ex. 1009 (“Chen”).

Thereof, and Products Containing the Same, Inv. No. 337-TA-1376; IPR2022-00618 (terminated due to settlement) and IPR2025-00004 (co-pending); and various related patents and patent applications. Pet. 4–6; Paper 5, 1–2.

III. ANALYSIS

A. *The Applicable Law*

To prevail in its challenges to patentability during trial, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). “In an IPR, 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) (2012) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion never shifts to the 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).

A patent claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter 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 ordinary skill in the art; and (4) when in evidence, objective

indicia of nonobviousness (also called secondary considerations), such as commercial success, long-felt but unsolved needs, and failure of others. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We analyze the challenges based on obviousness in accordance with the above-stated principles.

B. Level of Skill in the Art

Determining whether an invention would have been obvious under 35 U.S.C. § 103 requires resolving the level of ordinary skill in the pertinent art at the time of the effective filing date of the claimed invention. *Graham*, 383 U.S. at 17. The person of ordinary skill in the art is a hypothetical person who knows the relevant art. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Factors in determining the level of ordinary skill in the art include the types of problems encountered in the art, the sophistication of the technology, and educational level of active workers in the field. *Id.* One or more factors may predominate. *Id.*

Petitioner’s expert contends that person of ordinary skill in the art (POSITA):

[W]ould 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. Additional education could substitute for professional experience, or significant experience in the field could substitute for formal education.

Ex. 1003 ¶ 41. Patent Owner agrees with Petitioner’s expert regarding the level of ordinary skill in the art. RMTA 19. Patent Owner’s declarant, Dr. Villasenor, notes 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.” Ex. 2010 ¶ 19.

Based on a review of the record, we adopt Petitioner’s proposed level of ordinary skill in the art because it is consistent with the evidence of record, including the asserted prior art and ’178 patent specification. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

C. Claim Construction

In *inter partes* reviews, the Board interprets claim language using the district-court standard, as described in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). See 37 C.F.R. § 42.100(b). Under this standard, claim terms have their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the invention, in light of the language of the claims, the specification, and the prosecution history. See *Phillips*, 415 F.3d at 1313–14. Claim terms need only be construed to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

Petitioner states that “[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” Pet. 10. Patent Owner states that it “does not propose any specific claim constructions.” RMTA 19.

Nevertheless, the parties’ arguments raise issues regarding the scope of the claims of the ’178 patent which we discuss below.

D. Alleged Obviousness of Claims 1–6, 10, 12, 16–18, and 20 over Peterka

Petitioner challenges claims 1–6, 10, 12, 16–18, and 20 as obvious over Peterka. Pet. 18–50.

1. Peterka

Peterka, titled “Intial [sic] Free Preview For Multimedia Multicast Content,” was filed October 26, 2001, and published November 21, 2002. Ex. 1005, codes (54), (22), (43). Peterka is in part directed to offering free preview of a program to client computers in a multicasting system, allowing for the opportunity to decide whether to order the program content, and using encryption keys to distribute additional program content. *Id.* at code (57), ¶¶ 2, 6–7, 59, 83, 85. The encryption keys used to encrypt the program content are referred to as “Content Keys.” *Id.* ¶ 101. A content distribution system is made up of servers that download encrypted streaming media to clients. *Id.* at Fig. 1, ¶ 38.

Figure 7A, depicting the free preview approach, is reproduced below.

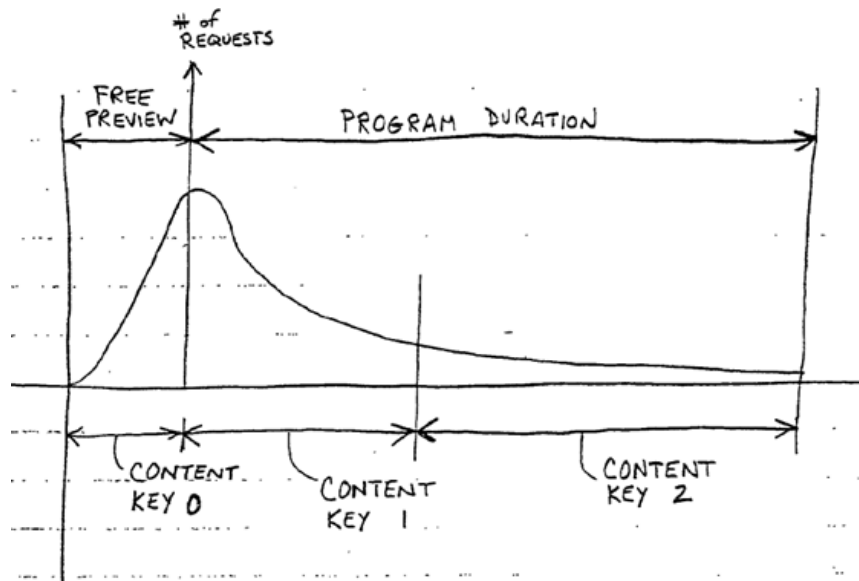


Figure 7A is a graph showing distribution of Content Keys during portions of a program, “showing the number of requests for a program versus the program duration.” Ex. 1005 ¶¶ 21, 91. During the “Free Preview” period during which client computers can “request an initial key for viewing an encrypted portion of the program.” *Id.* ¶¶ 91. For the Free Preview period, the content is encrypted with “Content Key 0,” which is freely distributed. *Id.* ¶¶ 91–92. Subsequent Content Keys are required to decrypt the remainder of the program content, delivered only to those clients that purchased the content. *Id.* ¶¶ 92–93. 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.* ¶ 93. 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.*

Figure 7B is reproduced below.

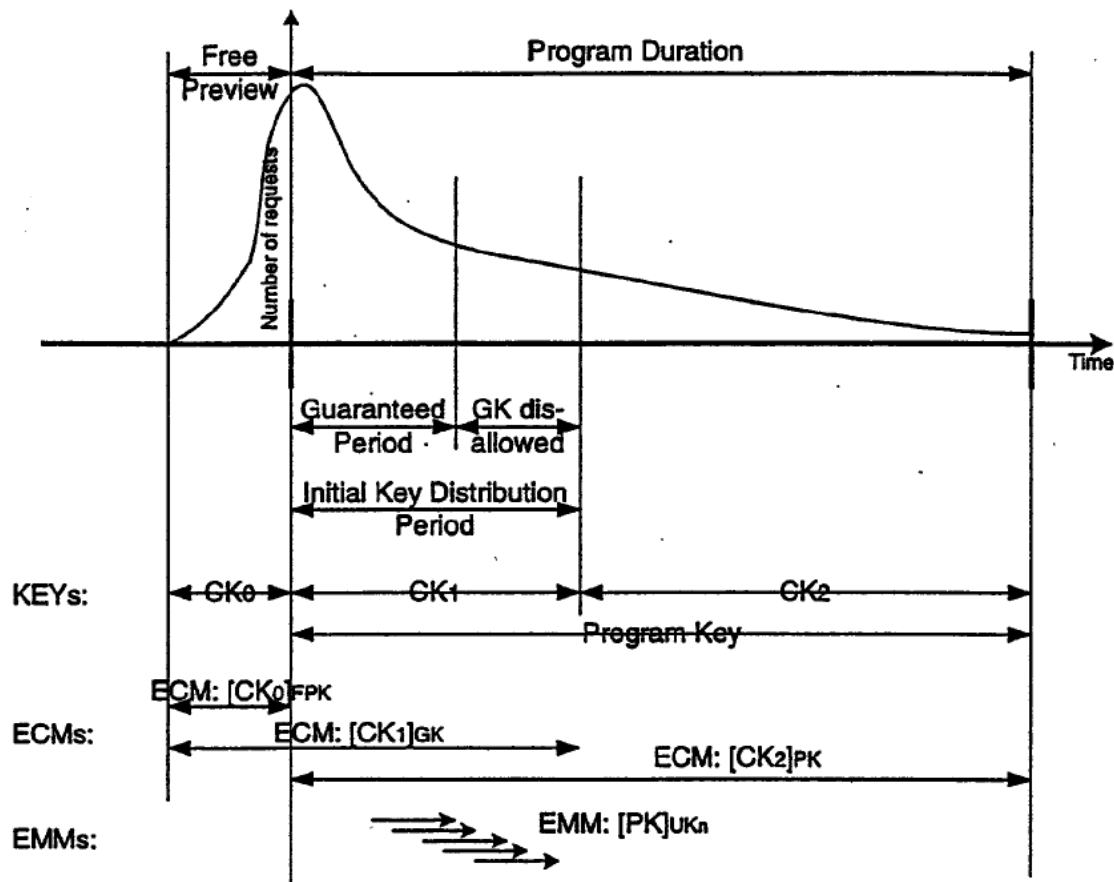


Fig. 7B

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 CK₂ 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.

One disclosed method of distributing content is a “Pay-By-Time” (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, provide for a “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 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. Independent Claims 1 and 16

a) Petitioner’s Challenge

For the preamble of claim 1, Petitioner relies on the disclosure in Peterka of supplying encrypted video content to clients. Pet. 19 (citing Ex. 1005, Figs. 1, 3, ¶¶ 12, 83, 94; Ex. 1003 ¶ 74).¹⁰

For the claim 1 requirement, “initiating a media playback request and receiving a playback request response,” Petitioner relies on the disclosure in Peterka of the ability of clients to purchase content and request encryption keys, and the response of servers in the form of Entitlement Management Messages (EMMs) or Entitlement Control Messages (ECMs). Pet. 19–22 (citing Ex. 1005, Figs. 7A, 7B, 8, 20A, 20B, ¶¶ 21, 80–82, 91–92, 104–106, 121–125, 130, 141–143; Ex. 1003 ¶¶ 75–81). In particular, Petitioner relies on the Pay-By-Time option, where “[w]hen the client negotiates encryption keys with the caching server, it will start receiving’ segments of selected ‘content’ from an ongoing show/event).” *Id.* at 19 (citing Ex. 1005

¹⁰ We make no determination whether the preamble of claim 1 (or of claim 16) is limiting.

¶¶ 80–82). Also, Petitioner relies on the free preview approach involving requests for programs and content keys, and the general description in Peterka of the methods for client requests for program content. *Id.* (citing Ex. 1005 ¶¶ 91–92, 141–143).

For the claim 1 requirement, “parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times,” Petitioner relies on the disclosure in Peterka of the content of the EMMs and ECMs, which messages, according to Petitioner’s expert, one of ordinary skill would have known would have been parsed by clients to extract the content. Pet. 23 (citing Ex. 1005, Fig. 7B, ¶¶ 104–106, 121–125; Ex. 1003 ¶¶ 82–84). In particular, Petitioner argues that the messages include the required content encryption keys, content encryption key identifiers, and content encryption key expiration times. *Id.* at 23–27 (citing Ex. 1005, Figs. 7B, 8, ¶¶ 80, 94–106, 121–122; Ex. 1003 ¶¶ 86–99).

As to the requirement that the content information includes content encryption keys, Petitioner argues that the playback request response of Peterka includes multiple keys and associated information. Pet. 20–22, 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 20 (citing Ex. 1005 ¶ 80; 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” *Id.* at 20–22 (citing Ex. 1005, Fig. 7B, ¶¶ 21, 53, 79–80, 121, 130; Ex. 1003 ¶¶ 78–79); *see also* Reply 4.¹¹

For the required expiration time element, Petitioner relies on Peterka’s disclosure that the messages contain “the time remaining in the lifetime of the key.” Pet. 26–27 (citing Ex. 1005 ¶ 121).

For the encryption key identifier requirement, Petitioner relies on the “sequence number or a time stamp,” contained in the messages, and argues that from the vantage point of one of ordinary skill, these items would have corresponded to, or made obvious, content encryption key identifiers. Pet. 25–26 (citing Ex. 1005, Fig. 7B, ¶¶ 80, 121–122; Ex. 1003 ¶¶ 90–96). 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.” *Id.* at 26 (citing Ex. 1003 ¶ 94). 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, Fig. 7B, ¶¶ 80, 122, 130; Ex. 1003 ¶¶ 93–96).

¹¹ 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. 22; PO Resp. 32.

For the claim 1 requirement, “retrieving content and manifest files from a content delivery server,” Petitioner relies on the disclosures in Peterka of clients receiving content from servers, and in addition argues that the use of manifest files in this context was a well-known way to provide information such as encoding methods. Pet. 28–31 (generally citing Ex. 1005; Ex. 1003 ¶¶ 102–110). Petitioner argues, “[m]anifests provided, e.g., ‘information about the encodings available from’ a media streaming system ‘and fragments stored by the system up to the current time,’ and other useful information that clients could access and use to help facilitate streaming.” *Id.* at 29 (citing Ex. 1003 ¶¶ 105–106). Petitioner supports its argument regarding manifest files by noting that Peterka provides for media to be “available at different ‘quality (i.e., bit rates)’ and describes the ‘server . . . adjust[ing] the rate in real time based on the immediate state of the network,’ and the ‘client . . . adjust[ing] the bit rate . . . in accordance with user selection.’” *Id.* at 30 (citing Ex. 1005 ¶ 54, 59, 119). Also, argues Petitioner, “it was conventional for content servers to (1) create manifest files with information regarding how a particular media segment is encoded (e.g., bit rates in multi-bit-rate streaming services) and (2) send such information to clients.” *Id.* (citing Ex. 1003 ¶¶ 104–110).

For the claim 1 requirement, “detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content,” Petitioner relies on the disclosure in Peterka of the above-discussed “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.” Pet. 31–33 (citing Ex. 1005, Figs. 7A, 7B, ¶¶ 80–82, 91–93, 105–106, 114,

122–125; Ex. 1003 ¶¶ 111–114). Petitioner also relies on the disclosure in Peterka of methods for signaling to the client information for the client to detect content encryption key rotation boundaries, such as including predetermined bit in the header of a packet sent from the server. *Id.* at 33–34 (citing Ex. 1005, Fig. 14, ¶¶ 105–106, 116–121; Ex. 1003 ¶¶ 115–117). Petitioner argues that this signaling provision is complementary to the pull model because it signals when to use keys, which would take place after the pull model causes a key request. *Id.*

For the claim 1 requirement, “issuing requests to a 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,” Petitioner relies on the above-referenced disclosure in Peterka of the “pull model,” in which the client requests a key distribution server for new keys before the current keys expire. Pet. 34–36 (citing Ex. 1005, Fig. 8, ¶¶ 105–106, 110; Ex. 1003 ¶¶ 118–122).

For the claim 1 requirement, “applying the second key for content decryption after the key rotation boundary is reached,” Petitioner relies on the disclosure in Peterka of receiving a new content encryption key and using that key to decrypt further content. Pet. 36–37 (citing Ex. 1005 ¶¶ 90, 92, 101, 105–106, 108, 110, 116; Ex. 1003 ¶¶ 123–124).

Independent claim 16 is a device counterpart to method claim 1, and Petitioner’s arguments and reliance on Peterka for this claim in substance track that for claim 1. Pet. 48–50 (citing Ex. 1003 ¶¶ 156–158).

b) Patent Owner’s Response

Patent Owner confines its arguments to three issues: that Peterka does not teach or suggest the independent claim 1 and 16 requirements of: (i) a

playback request response that includes multiple “content encryption keys”; (ii) a playback request response that includes “content encryption key identifiers”; and (iii) “detecting content encryption key rotation boundaries” and “issuing requests to a license server . . . to retrieve a second encryption key.” PO Resp. 1–3. We discuss these arguments in more detail below.

(1) Multiple “content encryption keys” requirement

Patent Owner relies on the fact that claims 1 and 12 require a playback request response that includes “content encryption keys,” thus requiring more than one key in the response. PO Resp. 6–7. For example, the ’178 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” Ex. 1001, 3:47–50. Patent Owner 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. PO Resp. 9 (citing Ex. 2010 ¶ 30).

Focusing on Petitioner’s reliance on the free preview/initial viewing approach of Figure 7B as implemented for the Pay-By-Time purchasing option,¹² 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 claims 1 and 16. PO Resp. 14–22, 26–27 (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

¹² 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 10–14; Reply 5–8.

advance, during a “provisioning” process, before there is any playback request or response. *Id.* Patent Owner submits that the only key in Figures 7A and 7B that is requested is CK₂, which is delivered only to those 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 ¶ 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 32–36 (citing Pet. 22, 28; Ex. 2010 ¶¶ 67–77).

(2) “Content encryption key identifiers” requirement

Patent Owner contends that Peterka’s teaching does not meet the limitation of “content encryption key identifiers.” PO Resp. 37–43. 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 37–38 (citing Ex. 2010 ¶¶ 82–83). Patent Owner bases this on the statement in the ’178 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 37 (citing Ex. 1001, 3:28–32).

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. 39–40 (citing Ex. 1005 ¶ 121; Ex. 2010 ¶¶ 89–90).

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. 40–43. 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 41 (citing Ex. 2010 ¶ 94). 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 41–42 (citing Ex. 2010 ¶¶ 94–95).

(3) “*Detecting content encryption key rotation boundaries*” and “*issuing requests*” requirements

Patent Owner argues that Petitioner’s reliance on Peterka’s 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,” fails to satisfy the claim requirement of “detecting content encryption key rotation boundaries between periods of use of different content encryption keys” PO Resp. 50–51 (citing Ex. 1005 ¶¶ 105–106; Ex. 2010 ¶¶ 117–118). Patent Owner premises this argument on a construction of the claims that requires detection of **both** key rotation boundaries that are based on key expiration times **and** those resulting from key change notifications, based on the description in the ’178 specification of the embodiments of the invention that detect both types of boundaries. *Id.* at 43–51 (citing Ex. 1001, Fig. 3, ¶¶ 1:63–65, 3:9–11, 3:46–47, 3:53–55, 9:47–49, 10:39–43, 10:65–11:7, 11:38–53; Ex. 2010 ¶¶ 100, 105, 107–109, 111, 114).

Patent Owner also relies on the claim 1 requirement that key expiration times are obtained by parsing information from the playback request response, which Patent Owner asserts “supports the conclusion that the claims’ separate requirement of ‘**detecting** content encryption key rotation boundaries’ is not met by identifying a key’s expiration time alone.” *Id.* at 48–49 (citing Ex. 2010 ¶ 112). Otherwise, argues Patent Owner, that “would render the ‘detecting’ limitation redundant to the ‘parsing’

limitation, which is disfavored.” *Id.* at 49 (citing *Power Mosfet Techs., L.L.C. v. Siemens AG*, 378 F.3d 1396, 1410 (Fed. Cir. 2004)).

Patent Owner also argues that Petitioner’s alternative reliance on the disclosure in Peterka of methods for signaling to the client information to detect content encryption key rotation boundaries, such as including predetermined bit in the header of a packet sent from the server, is unsound. PO Resp. 52–55. Patent Owner relies on the claim 1 requirement, “issuing requests . . . ahead of a key rotation boundary to retrieve a second content encryption key,” arguing that the signaling described in Peterka only alerts clients about keys that have already been provided, eliminating any suggestion that the key is requested in response to detecting the signaled key rotation boundary. *Id.* (citing Ex. 1005 ¶¶ 116–117; Ex. 2010 ¶¶ 120–126). Thus, argues Patent Owner, the disclosed signaling method only applies to the “push model” of Peterka, and would not have been obvious to adopt to the pull model. *Id.* at 54–55 (citing Ex. 2010 ¶¶ 127–128).

c) Petitioner’s Reply

(1) Multiple “content encryption keys” requirement

Petitioner in reply reiterates 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 4 (citing Pet. 20–22; Ex. 1005 ¶ 80; Ex. 1003 ¶¶ 77–79). Petitioner further relies on Peterka Figures 7A and 7B as 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.” Reply 7–8 (citing Pet. 20–22; Ex. 1003 ¶ 79). Petitioner explains 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 points out 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, argues Petitioner, “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.

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 12–14 (citing Ex. 1005, Fig. 7B, ¶¶ 21, 91, 122; Ex. 1003 ¶ 79). 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 14.

Petitioner also argues 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.

(2) “Content encryption key identifiers” requirement

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.* 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 ’178 patent. *Id.* at 21 (citing Ex. 1001, 3:34–35, 4:8–10).

Furthermore, Petitioner argues that the relied-on sequence numbers and time stamps are sufficient to uniquely identify the associated keys, as confirmed by Petitioner's expert's testimony citing background art in support. Reply 21–22 (citing Ex.1003 ¶¶ 93–96, 161–172, 201–221; Ex. 1041 ¶¶ 274–277). Petitioner also rejects 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 (citing PO Resp. 41–42).

(3) “Detecting content encryption key rotation boundaries” and “issuing requests” requirements

Petitioner argues that nothing in the intrinsic record justifies narrowing “detecting” from its ordinary meaning to exclude detecting key rotation boundaries that are period-based as shown in Figure 3 of the '178 patent. Reply 24.

Petitioner also argues that its reliance on Peterka's use of signals to detect content encryption key rotation boundaries is compatible with the Peterka pull key distribution method, because the pull method determines when to acquire new key and the use of signals determines the timing for when to apply the key, which can take place after the key is acquired. Reply 26 (citing Ex. 1005 ¶ 121; Ex. 1003 ¶¶ 33–34, 49).

d) Patent Owner's Sur-Reply

(1) Multiple “content encryption keys” requirement

Patent Owner 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. Rather, argues Patent Owner, Peterka states that only one key is requested during a segment, which key is for the next segment. *Id.* (citing Ex. 1005 ¶ 80).

Patent Owner repeats 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 ¶ 54). 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.

Patent Owner focuses on a statement by Petitioner that “**Every element** of claims 1 and 16 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 3–5 (citing Pet. 18; Ex. 1005, Fig. 8, ¶110; Ex. 2010 ¶¶ 55–56). 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 7–8. Patent Owner argues that “the

Petitioner'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.

In regard to 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 13. 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.

(2) “Content encryption key identifiers” requirement

Patent Owner argues that the statement in the ’178 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, 3:29–32; *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. Sur-Reply 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.

(3) *"Detecting content encryption key rotation boundaries" and "issuing requests" requirements*

Patent Owner reiterates its position that, based on Figure 3 and its accompanying description in the '178 specification, "detecting content encryption key rotation boundaries" requires "checking a key's expiration time **and** checking for an explicit key change notification." Sur-Reply 21–23.

Regarding Petitioner's reliance on Peterka's key change notifications, Patent Owner again argues that there is no disclosure in Peterka of clients issuing requests for keys in response to a key change notification — rather, any key associated with a notification has already been provided to the client. Sur-Reply 23–26. Patent Owner explains that it is the server that generates the notification, but for Peterka's pull model, "the server need not monitor the status of the client's keys[.]" *Id.* at 23–24 (citing Ex. 1005 ¶ 116). Patent Owner explains that its objection to Petitioner's position is not that the "detecting" requirement must precede the "issuing requests" requirement, but rather that Peterka fails to teach "doing *both* within the same embodiment." *Id.* at 24. Specifically:

Peterka fails to do so because when Peterka provides a key change notification, it *also* provides the new key without the client issuing any request for that key, and when Peterka's client requests a new key through its pull model, it *only* does so because of an upcoming expiration time, and never because of a key change signal.

Id.

e) Analysis

We are not persuaded by Patent Owner's arguments that Peterka fails to teach or suggest the independent claim 1 and 16 requirements of a playback request response that includes multiple "content encryption keys" and "content encryption key identifiers," and the requirements of "detecting content encryption key rotation boundaries" and "issuing requests to a license server . . . to retrieve a second encryption key.

(1) Multiple "content encryption keys" requirement

Contrary to Patent Owner's assertion that Petitioner raises new arguments in its Reply, Petitioner has consistently relied 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, 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.¹³ Ex. 1005, Fig. 7B, ¶¶ 80–82. This tracks the disclosed embodiment of the '178 patent, in which the initial request for playback provides the current content encryption key and the next future content encryption key, followed by successive requests for subsequent keys before key rotation boundaries occur. Ex. 1005, Fig. 3, 3:47–50.

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. *E.g.*, 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. (It is irrelevant that the FPK and GK keys are provisioned in advance—those keys are simply used in the ECMs to encrypt CK₀ and CK₁, respectively.) Moreover, Patent Owner has no basis 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. Apparently Patent Owner assumes

¹³ 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.

that a free preview simply occurs due to some unknown agency without any client request — we see no support in Peterka for that speculation.

We are also 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, that statement supports the fact that CK_0 , which is key for the initial free preview period, and CK_1 , 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 CK_0 and CK_1 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” requirement

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 ’178 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.” Ex. 1001, 3:29–32. Immediately after that statement, 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, 3:32–36. We do not see how Peterka’s “sequence number or a time stamp” differs in any pertinent respect from the ’178 patent’s “wall clock time” or “segment number.” Likewise, we do not agree that the fact that Peterka includes the sequence number or time stamp in the EMM or ECM message along with the key somehow fails to satisfy the ’178 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. Sur-Reply 19. There is simply no basis for that assertion. (Again, the fact that CK₀ is encrypted with the FPK key and CK₁ is encrypted with the GK key does not support Patent Owner’s assertion).

(3) “Detecting content encryption key rotation boundaries” and “issuing requests” requirements

We determine that the claim requirements, “detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content,” and “issuing requests to a 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,” are satisfied by Peterka’s pull method of key management. The pull method of Peterka corresponds to the detection of key rotation boundaries that are period-based, and resulting key rotation, as

shown in Figure 3 of the '178 patent. Although Figure 3 and accompanying description also describe detection of boundaries resulting from key change notifications, there is no reason to require the complete description of the Figure 3 embodiment to be incorporated into the requirements of the claims. The claims do not require detection of boundaries resulting from key change notifications. *See Superguide Corp. v. DirecTV Enter., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (“a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment”).

Regarding Petitioner’s alternative reliance on the provision in Peterka of signaling to the client the availability of new content encryption key via, for example, including a predetermined bit in a header, we agree with Petitioner that this feature can be used in a pull model of key management, and therefore is a reasonable alternative way to provide for detection of key rotation boundaries.

(4) Summary

Based on the above analysis, and on our further review of Petitioner’s reliance on Peterka’s disclosures in challenging the remaining requirements of claims 1 and 16, having considered and weighed the entirety of the evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 1 and 16 are unpatentable under 35 U.S.C. § 103(a) over Peterka.

3. Claims 2–6, 10, 12, 17, 18, and 20

Claim 2 adds to claim 1 the requirement that “the playback request response include the content encryption key and associated identifier currently being applied as well as a future content encryption key and

associated identifier yet to be applied.” Ex. 1001, 12:23–27. Claim 17 adds a commensurate limitation. *Id.* at 14:12–17. Petitioner relies on a statement in Peterka describing providing “keys to the current as well as the next segment.” Pet. 37, 50 (citing Ex. 1005, Fig. 7B, ¶¶ 80, 130; Ex. 1003 ¶¶ 125, 159).

Claim 3 adds to claim 1 the requirement that “the content encryption key expiration returned in the playback request response is expressed as an expected minimum interval between periodic key rotation,” and claim 4 adds to claim 3 the requirement of “timing the prefetching of a next un-retrieved content encryption key based on an expected expiration of the content encryption key currently being used.” Ex. 1001, 12:28–36. Claim 18 adds a limitation commensurate to claim 4. *Id.* at 14:18–22. Petitioner relies on the disclosure in Peterka that media streams can be divided into “purchasable segments” to allow users to pay for content by the amount of time (segments) of the stream that the user consumes, that segments have a defined period that yields “periodic key rotation,” and that that key distribution messages identify the expiration time of the key provided in the message. Pet. 38–39 (citing Ex. 1005, Fig. 8, ¶¶ 78–82, 99–101, 105–106, 110, 121; Ex. 1003 ¶¶ 126–129). Petitioner’s expert opines that, in view of these disclosures, it would have been obvious that the disclosed expiration times constituted a minimum interval during which the key was expected to be used between periodic key changes. Ex. 1003 ¶ 130. For claims 4 and 18, Petitioner further relies on the disclosure in Peterka that “each client keeps track of the keys and their expiration times and actively requests new keys before the current keys expire.” Pet. 41, 50 (citing Ex. 1005 ¶¶ 82, 105–106; Ex. 1003 ¶¶ 135–136, 159).

Claim 5 depends from claim 4 and additionally requires “prefetching a next un-retrieved key a fixed duration before the expected expiration of the content encryption key currently being used.” Ex. 1001, 12:37–39.

Petitioner argues that adopting such fixed key retrieval time was a conventional, straightforward choice that would help predictability and avoid service interruptions. Pet. 41–42 (citing Ex. 1005 ¶¶ 105, 121; Ex. 1003 ¶¶ 137–140).

Claim 6 requires:

The method of claim 4, further comprising: prefetching a next un-retrieved key within a period of time after the expected expiration of the content encryption key currently being applied, the period of time beginning at the expected expiration of the content encryption key currently being used, and ending at a duration calculated as a fixed percentage of a fixed periodic content encryption key expiration interval.

Ex. 1001, 12:40–46. Petitioner relies on the fact that, in Peterka, a second key is acquired in a first segment before a first key expires, and in the next segment, a third key is acquired before the second key expires, thus satisfying the timing relationships of the claim, because the third key is prefetched during the second segment after the first key expires. Pet. 43–45 (citing Ex. 1005 ¶¶ 82, 105–106, 110; Ex. 1003 ¶¶ 141–147). Petitioner argues that using a fixed percentage of the fixed periodic expiration interval would have been an obvious implementation choice. *Id.*

Claim 10 adds to claim 1 the requirement, “wherein license server communications are secured and authenticated using a selected one of Secure Sockets Layer and a token-based technique using a token encrypted with a symmetric key.” Ex. 1001, 12:59–62. Petitioner relies on the disclosure in Peterka of requiring authentication of clients, in combination

with the fact that Secure Sockets Layer and symmetric key token-based techniques were well known. Pet. 45–47 (citing Ex. 1005, Figs. 19–21, ¶¶ 4, 15, 38, 66, 75, 135–136, 142–144, 146; Ex. 1003 ¶¶ 148–153).

Claim 12 adds to claim 1 the requirement that “actual content encryption key rotation boundaries are detected based on real-time in-band notifications.” Ex. 1001, 12:65–67. Claim 20 is commensurate. *Id.* at 14:26–28. For these claims, Petitioner relies on the disclosure in Peterka of a client checking content packets for a signal to start applying a new key. Pet. 48, 50 (citing Ex. 1005, Fig. 14, ¶¶ 116–121; Ex. 1003 ¶¶ 154–155, 159).

Other than its arguments directed to Petitioner’s challenges to the independent claims, Patent Owner does not specifically respond to Petitioner’s arguments regarding dependent claims 2–6, 10, 12, 17, 18, and 20. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. Accordingly, based on the above analysis, having considered and weighed the entirety of the trial record and evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 2–6, 10, 12, 17, 18, and 20 are unpatentable under 35 U.S.C. § 103 over Peterka.

E. Alleged Obviousness of Claims 1–6, 10, 12, 14, 16–18, and 20 over Peterka, Suzuki and Bocharov

Petitioner challenges claims 1–6, 10, 12, 14, 16–18, and 20 over the combination of Peterka, Suzuki and Bocharov. Pet. 66–68.¹⁴

¹⁴ Petitioner also challenges claims 1–6, 10, 12, 16–18, and 20 over the combination of Peterka and Suzuki, and challenges claims 1–6, 10, 12, 14, 16–18, and 20 over the combination of Peterka and Bocharov. Pet. 50–65.

1. Suzuki

Suzuki is a Japanese patent application publication titled “Key Exchange Method in Multicast Distribution System.” Ex. 1006, code (54).

Suzuki’s object is to:

[P]rovide 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.

Ex. 1006 ¶ 11. Suzuki describes a multicast distribution system with a content server and a key management server, wherein:

[T]he 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)

. . . .

[T]he 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)

. . . .

[T]he key management server “creates the encryption key/decryption key to be used next in response to the key

Given our determination regarding Petitioner’s challenge based on the combination of Peterka, Suzuki and Bocharov, it is unnecessary to specifically address these alternative challenges, other than to the extent the arguments raised and record cited in the Peterka/Suzuki and Peterka/Bocharov challenges are relied on for the Peterka/Suzuki/Bocharov challenge.

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.

2. *Bocharov*

Bocharov is titled “Delivering Cacheable Streaming Media Presentations.” Ex. 1007, code (54). Bocharov is directed to streaming media fragments from a server to clients, including providing manifest files containing metadata information about the fragments. *Id.* at code (57), Fig. 5, ¶¶ 30–31, 53. The manifest can provide timestamps for each fragment archived up to the point of the request, and the client uses the timestamp to compose a URL for requesting the fragment from the server. *Id.* ¶¶ 30–31.

3. *The Combination of Peterka, Suzuki, and Bocharov*

Petitioner argues that one of ordinary skill would have had reason to combine the teachings of Peterka, Suzuki, and Bocharov. Pet. 51–53, 57–59, 66–67. Petitioner argues that Suzuki, like Peterka, discloses clients acquiring keys for multiple media segments, and provides implementation details, not disclosed in Peterka, regarding how to keep track of keys and their expiration times, and how to determine when a new key is required. Pet. 51–52 (citing Ex. 1003 ¶¶ 161–164). Petitioner argues that, given that Peterka and Suzuki are in the same field of art, one of ordinary skill would

have been motivated to use the specific details of Suzuki in implementing the disclosure of Peterka. *Id.* at 53, 66 (citing Ex. 1003 ¶¶ 165–167, 202–204).

Petitioner also argues that Peterka indicates that video content can be streamed using various protocols and bit rates, but does not provide implementation details. Pet. 57–59, 66–67 (citing Ex. 1003 ¶¶ 179–184, 204). However, argues Petitioner, one of ordinary skill in the art would have had reason to use the manifest files of Bocharov to provide the necessary information to handle different protocols and bit rates. *Id.* Petitioner argues that one of ordinary skill in the art would have been so motivated because implementing Peterka’s system to use Bocharov’s manifests would have provided an effective solution for allowing clients to switch between multiple versions of a media program having different encodings/qualities/bit rates. *Id.*

Patent Owner argues that there was no motivation to combine Peterka with Suzuki because Petitioner has argued that “Peterka can ***already*** identify content keys by ***using*** the allegedly unique sequence numbers or time stamps assigned to each ***message*** carrying a single content key.” PO Resp. 41–42 (citing Pet. 25). Patent Owner also challenges motivation to combine Suzuki because it “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.” *Id.* at 36–37. Petitioner responds that, because Peterka disclosed alternative embodiments that did not use sequence numbers or time stamps to identify EMM/ECM messages, one of ordinary skill would have been motivated specifically assign identifications to individual keys as

taught in Suzuki. Reply 22 (citing Pet. 26). Petitioner also argues that whether Suzuki was directed to unpurchased content was irrelevant, because Suzuki is cited to show multiple key responses were conventional. *Id.* at 19–20.

Patent Owner does not otherwise specifically address the issue of motivation to combine Peterka, Suzuki, and Bocharov. *See generally* PO Resp. Nonetheless the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. We find, based on the record, that Petitioner has proved by a preponderance of the evidence that a person of ordinary skill in the art would have had reason to combine the teachings of Peterka, Suzuki, and Bocharov as proffered by Petitioner with a reasonable expectation of success.

4. Claims 1–6, 10, 12, 14, 16–18, and 20

In addition to referencing the arguments and record marshaled for Petitioner’s challenges to claims 1–6, 10, 12, 16–18, and 20 based on Peterka alone, Petitioner relies on the teachings of Suzuki in combination with Peterka to additionally argue the obviousness of the claim 1 and claim 16 requirement of “content encryption key identifiers” in a “playback request response,” and the timing requirements for the “prefetching” recited in claims 4–6 and 18. Pet. 54–57, 67–68 (citing Ex. 1003 ¶¶ 168–176, 205–207).

Likewise, Petitioner relies on the teachings of Bocharov in combination with Peterka to additionally argue the obviousness of the claim 1 and claim 16 requirements of retrieving manifest files from a content delivery server, and the claim 12 and 20 requirement of the actual content

encryption key rotation boundaries detected based on real-time in-band notifications. Pet. 60–64, 67–68 (citing Ex. 1003 ¶¶ 185–197, 205–207).

Claim 14 adds to claim 12 the requirement that “content encryption key rotation boundaries are detected based on notifications present in the content manifest file, the content manifest file being selected from an m3u8 file, an IIS Smooth Streaming manifest file, a DASH MPD file and a proprietary manifest file.” Ex. 1001, 13:4–9. Petitioner relies on the disclosure in Bocharov that its manifest file can be an Internet Information Server (“IIS”) smooth streaming manifest file. Pet. 64–65 (citing Ex. 1003 ¶¶ 198–200).

In addition to its arguments directed to Petitioner’s challenges to the independent claims based on Peterka alone, Patent Owner also argues that Suzuki does not teach “transmitting multiple ‘*content encryption keys*,’ [it] only disclose[s] providing ‘key *information* relating to the key currently in use (key A) and the next key to be used (key B).’” PO Resp. 36 (citing Ex. 1006 ¶¶ 76–77; Ex. 2010 ¶ 78). Petitioner responds that Suzuki “uses the term ‘key information’ to mean *both* ‘the key’ itself ‘and associated information’ such as key number and remaining validity time,” that Suzuki responds to client requests by sending key information relating to the key currently in use and the next key to be used, and that Suzuki shows multiple keys transmitted in a single response message, along with the keys’ key numbers and remaining validity times. Reply 18–19 (citing Ex. 1006, Figs. 5, 6, ¶¶ 12, 50, 72–73, 76–77, 119; Ex. 1003 ¶ 81). We find that Petitioner’s reliance on Suzuki is sound.

Patent Owner does not otherwise specifically respond to any of Petitioner’s other arguments regarding claims 1–6, 10, 12, 14, 16–18, and 20

as obvious over Peterka, Suzuki, and Bocharov. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. Accordingly, based on our analysis set forth above, having considered and weighed the entirety of the evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 1–6, 10, 12, 14, 16–18, and 20 are unpatentable under 35 U.S.C. § 103(a) over the combined teachings of Peterka, Suzuki, and Bocharov.

F. Alleged Obviousness of Claims 7, 8, and 19 over Peterka, Bocharov, Peterka308, and Chen

Petitioner challenges claims 7, 8, and 19 as obvious over the combination of Peterka, Bocharov, Peterka308, and Chen. Pet. 69–73.

Peterka308, titled “Method And Apparatus For Providing A Secure Trick Play,” was filed August 22, 2007, and published October 30, 2008. Ex. 1008, codes (54), (22), (43). Peterka308 is directed to encrypting video segments, with expiration times for the encryption keys to place a time limit on playability of the content, and the use of stored timestamps to generate keys rather than storing the keys themselves. *Id.* at code (57), ¶¶ 24–28.

Chen, titled “Method and system for encrypting material for distribution,” was filed October 29, 2003, and published May 12, 2004. Ex. 1009, codes (54), (22), (43). Chen is directed to encrypting video segments, with the time periods for each encrypted segment based on (i) fixed time intervals, (ii) a fixed number of packets, (iii) a fixed marker count, or (iv) a pseudo random number of packets. *Id.* at code (57), Figs. 2A–2D, ¶¶ 8, 10, 34.

Petitioner argues that that one of ordinary skill would have been motivated to improve the Peterka/Bocharov combination with Peterka308 and Chen in order to expand the single-bit key identification approach of Peterka to accommodate multiple keys, including the advance distribution of keys, by using the time stamp approach of Peterka308 and the methods for determining segment periods in Chen. Pet. 69–71 (citing Ex. 1003 ¶¶ 209–215). Patent Owner does not specifically respond to this argument. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. We find, based on the record, that Petitioner has proved by a preponderance of the evidence that a person of ordinary skill in the art would have had reason to combine the teachings of Peterka, Bocharov, Peterka308, and Chen as proffered by Petitioner with a reasonable expectation of success.

Claim 7 requires “subsequent content encryption key identifiers are predictable based on a predetermined known progression.” Ex. 1001, 12:47–49. Claim 19 is commensurate in scope. *Id.* at 14:23–25. Claim 8 additionally requires the identifier to be calculated as monotonically increasing sequential integer values based on the number of segments or video frames generated during a fixed periodic content encryption key expiration interval. *Id.* at 12:50–54. For these claims, Petitioner relies on the timestamp disclosures of Peterka308 and the techniques for segmenting media content of Chen. Pet. 72–73 (citing Ex. 1008 ¶¶ 24, 29, 32; Ex. 1009, Figs. 2A–2C, ¶¶ 34–44; Ex. 1003 ¶¶ 216–221).

Other than its arguments directed to Petitioner’s challenges to the independent claims based on Peterka alone, Patent Owner does not specifically respond to any of Petitioner’s arguments regarding dependent

claims 7, 8, and 19. *See generally* PO Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Accordingly, based on the above analysis, and on our further review of Petitioner’s reliance on Peterka’s disclosures in challenging the remaining requirements of claims 1 and 16, having considered and weighed the entirety of the evidence, we determine that Petitioner has proved by a preponderance of the evidence that claims 7, 8, and 19 are unpatentable under 35 U.S.C. § 103 over the combined teachings of Peterka, Bocharov, Peterka³⁰⁸, and Chen.

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 proposed 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 21–37 in one-to-one correspondence with the set of original claims 1–8, 10, 12–14, 16–20. RMTA Claims App’x.¹⁵ Of the proposed substitute claims, claims 21 and 33 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] initiating a media playback request and receiving a
playback request response;

[21.2] parsing content information from the playback request
response, the content information including content
encryption keys, content encryption key identifiers each
assigned to an associated content encryption key, and
content encryption key expiration times, said content
encryption key identifiers each uniquely identifying
each associated content encryption key from every
other content encryption key for the entire duration of a
media playback, said media playback corresponding to
the media playback request response;

[21.3] retrieving content and manifest files from a content
delivery server;

[21.3A] applying a first key for content decryption, said first
key having a first expiration time defining a time-based
content encryption key rotation boundary;

[21.4] detecting a notification, the notification including a
notification-based content encryption key rotation

¹⁵ Patent Owner proposes substitute claim 31 for original claim 13. RMTA Claims App’x iv. However, Petitioner does not challenge claim 13. Therefore, this proposed amendment is improper for this reason alone.

boundary between periods of use of different content encryption keys in decrypting retrieved content, wherein the notification requires expiration of said first content encryption key earlier than said time-based content encryption key rotation boundary for said first key and after said notification-based content encryption key rotation boundary for said first key;

[21.5] issuing requests to a license server in response to detecting said notification-based content encryption key rotation boundary ahead of a said time-based content encryption key rotation boundary for said first key to retrieve a second content encryption key to be used after a the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached; and

[21.6] applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said first key is reached.

RMTA 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. RMTA 6 (citing 37 C.F.R. § 42.121(a)(3)). Petitioner does not address this factor. *See generally* Opp. RMTA. 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. RMTA 4–5. 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. RMTA. With the exception of substitute claim 31, which purports to amend unchallenged claim 13, 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.” RMTA 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.

However, Petitioner argues 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 one “key rotation boundary” (hereafter, “**Boundary**”) and required two actions relative to that claimed **Boundary**: (1) “issuing requests to a license server *ahead of* a [**Boundary**] to

retrieve a second [CEK]” and (2) “applying the second key for content decryption *after* the [**Boundary**] is reached.”

Opp. RMTA 2. Petitioner refers to this requirement as an “‘ahead of/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] **issuing requests** to a license server *in response to detecting* said **notification-based [CEK] rotation boundary ahead of** said **time-based [CEK] rotation boundary** for said first key to retrieve a second [CEK]...;

and

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

Opp. RMTA 3 (citing RMTA Claims App’x, ii) (emphasis supplied by Petitioner). Petitioner argues that claim 21 “do[es] not preserve the same sequence of (1) issuing requests ***ahead of a Boundary*** and (2) applying a second CEK ***after that same Boundary***. *Id.* This is so, argues Petitioner, because the request to retrieve the second key is made “in response to” detecting the notification-based boundary, rather than made ahead of that boundary. *Id.* Thus, for the notification-based boundary, the substitute claims are not limited to the “ahead of/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 “ahead of/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 request to retrieve the second key is made “in response to” detecting the notification-based boundary necessary means that the request must also occur before the notification-based boundary. Reply RMTA 3. Patent Owner states, “the second CEK must be requested ‘in response to’ ***detecting*** that upcoming boundary, and thus ***before*** that boundary.” *Id.* at 4. Patent Owner also argues that the timing of requesting and applying the second key in relation to the time-based boundary is not relevant, because the proper focus is on the notification-based boundary. *Id.*

Petitioner replies that there is no basis for Patent Owner’s assumption that the claims require the second key to be requested in response to detecting notifications of an “upcoming” boundary. Sur-Reply RMTA 2–3. Instead, argues Petitioner, the notification of the boundary can occur at the time the boundary occurs, or even afterwards, given that the ’178 patent describes notifications of boundaries that are not “upcoming.” *Id.* (citing Ex. 1001, 4:13–15, 7:20–24, 7:53–63, 9:4–6, 10:43–65, 11:5–15).

Furthermore, argues Petitioner, even if the notification of the boundary occurs before the boundary, the request that is made in response to detecting that notification 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 the key request to be made “in response to detecting” the boundary, rather than “ahead of” the boundary,

the request can occur before or after the boundary. This is not a fanciful or unlikely possibility — such delayed requests are specifically contemplated by the '178 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, 6:32–37.

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, 8:9–11.

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, 9:1–4.

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

Ex. 1001, 11:18–20.

Therefore, based on our review of the record, we conclude that Patent Owner has not made 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 '178 Patent. RMTA 6–10. 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 6 (citing '178 Patent Application Publ. No. 2014/0237243 (“the '243 Publication,” Ex. 2007); U.S. provisional app. 61/500,316 (“the Provisional Application,” Ex. 2008); U.S. Patent Application Publ. No. 2012/0331293 (Ex. 2009)). In particular, Patent Owner addresses claim support issues raised by Petitioner in its opposition to the original motion to amend (Paper 28), and discussed in our Preliminary Guidance (Paper 30), regarding the “content encryption key identifiers,” “issuing requests to . . . retrieve a second content encryption key,” and “applying the second key” claim requirements. *Id.* at 10–13.

Petitioner in opposition renews its contention that the original disclosure still does not support the “applying the second key” claim requirements in their current form — specifically, the substitute claim 21.6 requirement, “applying the second key for content decryption after the notification-based content encryption key rotation boundary for said first key and before said time-based content encryption key rotation boundary for said

first key is reached,” and the commensurate requirement of substitute claim 33. 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 ’243 Publication on which Patent Owner relies (Ex. 2007, Fig. 3, ¶¶ 5, 36, 39) 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. 2008, Fig. 3 (steps 304, 308), pp. 11–12).¹⁶ 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

¹⁶ Patent Owner asserts that the other priority documents (Exhibits 2007 and 2009) have the same disclosures as the Provisional Application. Reply RMTA 7.

“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. 2008, 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:

The ’243 publication describes circumstances in which “a key change is signaled . . . outside of any fixed duration lifespan” for security reasons (Ex. 2007 ¶ 35) 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.* ¶ 36).

Paper 30 at 9. 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. Ground 6A: Alleged Obviousness of Claims 21–26, 29, 30, 33–35, and 37 over Peterka and Traw

Petitioner challenges substitute claims 21–26, 29, 30, 33–35, and 37 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 includes 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. 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 record, that Petitioner has proved by a preponderance of the evidence that a person of ordinary skill in the art would have had reason to combine Peterka with Traw as proffered by Petitioner with a reasonable expectation of success.

3. *Substitute Claims 21 and 33*

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 33, Petitioner relies on its arguments for original claim 16 and substitute claim 21. *Id.* at 23 (citing Ex. 1047 ¶ 397).

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

a) Limitation [21.2]

Petitioner contends Peterka teaches content encryption key identifiers requirements of claim limitation [21.2] by describing delivering a sequence number or timestamp to a client along with a 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 ¶¶ 0121; Ex. 1003 ¶¶ 91–92; Ex. 1041 ¶¶ 274–277). Petitioner points out that the encryption key identifiers in the ’178 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, 3:34–35, 4:8–10, 6:1–4, 6:17–19; Ex. 1047 ¶¶ 347–349); 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. 26; Ex. 1042, 3:32–46, 4:45; Ex. 1003 ¶¶ 93–96; Ex. 1047 ¶¶ 350–356); Sur-Reply RMTA 9.

In addition, 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 14 (citing Ex. 1005 ¶ 121; Ex. 1047 ¶ 353).

Alternatively, Petitioner argues that 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 (citing Ex. 1005, Figs. 7A, 7B, ¶ 92; Ex. 1003 ¶¶ 94–96; Ex. 1047 ¶¶ 354–356).

Also, Petitioner contends a person of ordinary skill in the art would have understood that Peterka’s “media playback” also “correspond[s] to the media playback request response,” because the encryption codes Peterka’s client receives when it first requests/negotiates access to media content are used to decrypt and play back the media content the client sought access to. Opp. RMTA 15 (citing Pet. 19–22; Ex. 1047 ¶ 357).

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 ¶¶ 89, 93–95); *see* RMTA 14–15. We are not persuaded by these arguments for the reasons discussed in Section III.D.2.e)(2) above.

b) Limitation [21.3A]

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 ¶ 97; Ex. 1047 ¶¶ 360–362).

c) Limitation [21.4]

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 16–17 (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 ¶¶ 364–366).

d) Limitation [21.5]

For the “issuing requests . . . to retrieve a second content encryption key” 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, 110; Ex. 1042, 2:43–64, 3:17–19, 4:63–65, 5:35–65, 6:12–21, 6:39–57; Ex. 1047 ¶¶ 367–377).

In reply, Patent Owner argues that Petitioner does not identify any teaching in Peterka or Traw of a client requesting a new key in response to a key change notification. Reply RMTA 9; *see* RMTA 16–17. Patent Owner repeats its argument that the signaling described in Peterka only alerts clients about keys that have already been provided, rather than causing a key request in response to detecting the signaled key rotation boundary. *Id.* at 9–10 (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. 1042, 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. 1042, 2:43–64, 5:8–12, 5:27–33, cl. 1; Ex. 1047 ¶¶ 374–375). Petitioner also argues that Patent Owner fails to refute that parsons 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 ¶ 124; Ex. 1047 ¶ 379).

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

e) Limitation [21.6]

For the “applying the second key” requirement of claim 21, Petitioner argues that a person of ordinary skill would have been motivated to implement the Peterka/Traw combination to minimize service interruptions, such that when the client receives the second (replacement)

key due to Traw's unscheduled key revocation, , the client promptly applies the second key for decryption, before the current key is set to expire. Opp. RMTA 19 (citing Ex. 1005 ¶¶ 105–106, 116; Ex. 1042, 3:17–19, 4:63–65, 5:35–39, 5:63–65, 6:12–21, 6:39–57; Ex. 1003 ¶ 124; Ex. 1047 ¶¶ 378–379).

f) Claims 21 and 33 Summary

Other than Patent Owner's arguments directed to limitations 21.2 and 21.5 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 33 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 33 would be unpatentable under 35 U.S.C. § 103(a) over the combination of Peterka and Traw.

4. Substitute Claims 22, 23, 30, 34, 35, and 37¹⁷

Substitute claims 22, 23, 34, and 35 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 (claims 22 and 34) or to the first key's original expiration time plus its remaining time when it was expired (claims 23 and 35). Petitioner argues that both of these expiration time options were obvious to try based on practical considerations such as accommodating already-staged key

¹⁷ For substitute claims 24–26 and 29, Petitioner relies on its challenges of claims 4–6 and 10 as obvious over Peterka. Opp. RMTA 22–23 (citing Pet. 41–47; Ex. 1047 ¶¶ 392, 397).

rotation boundaries tied to future media segments and handling potential latency issues. Opp. RMTA 20–23 (citing Pet. 37–41; Ex. 1005, Fig. 7B, ¶¶ 80, 122; Ex. 1042, 3:35, 4:45; Ex. 1047 ¶¶ 380–391, 397).

Patent Owner argues that Petitioner’s argument that the expiration time requirement of claim 23 (and claim 35) would have been obvious to try is unsound because it relies on an open-ended selection or possible choices. RMTA 17–18; Reply RMTA 11–12. However, we agree with Petitioner 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 ¶¶ 390–391).

Substitute claims 30 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. 1042, Fig. 2, 1:65–2:2, 2:15–19, 3:65–66, 4:37–39, 5:5–39; Ex. 1047 ¶¶ 393–397).

Patent Owner argues, for claim 30 (and claim 37), 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 18; Reply RMTA 12. However, we agree with Petitioner 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 ¶¶ 396–396).

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 22–26, 29, 30, 34, 35, and 37 are unpatentable under 35 U.S.C. § 103(a) over the combination of Peterka and Traw.

F. Grounds 6B–6E: Alleged Obviousness of Claims 21–30 and 32–37

Petitioner also contends persons of ordinary skill in the art would “have combined Traw with the original grounds set forth in the Petition (Grounds 2–5), for the same reasons” discussed above (Opp. RMTA 24 (citing *id.* § II.A.3; Ex. 1047 ¶ 398)), and argues that those combinations “meet substitute claims 21–26, 29–30, 33–35, and 37 for the same reasons discussed *supra* §§II.A.4–II.A.9, **and also** meet substitute claims 27–28, 32, and 36 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. 51–55, 66–68; Ex. 1005, Figs. 7A, 7B, ¶ 92; Ex. 1006, Fig. 2, ¶¶ 13, 30, 43–48, 80; Ex. 1003 ¶¶ 161–172, 201–207; Ex. 1047 ¶¶ 399–402).

Patent Owner generally relies on its arguments for Ground 6A, discussed above, 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 21–30 and 32–37 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. CONCLUSION¹⁸

For the foregoing reasons, we are persuaded that Petitioner establishes by a preponderance of the evidence that claims 1–8, 10, 12, 14, and 16–20 of the '178 patent have been shown to be unpatentable.

In summary:

Claims	35 U.S.C. §	References/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–6, 10, 12, 16–18, 20	103	Peterka	1–6, 10, 12, 16–18, 20	
1–6, 10, 12, 16–18, 20	103	Peterka, Suzuki ¹⁹		
1–6, 10, 12, 14, 16–18, 20	103	Peterka, Bocharov ²⁰		
1–6, 10, 12, 14, 16–18, 20	103	Peterka, Suzuki, Bocharov	1–6, 10, 12, 14, 16–18, 20	

¹⁸ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. §§ 42.8(a)(3), (b)(2).

¹⁹ We do not reach this challenge to claims 1–6, 10, 12, 16–18, and 20 given our determination regarding Petitioner's challenge to these claims based on the combination of Peterka, Suzuki and Bocharov.

²⁰ We do not reach this challenge to claims 1–6, 10, 12, 14, 16–18, and 20 given our determination regarding Petitioner's challenge to these claims based on the combination of Peterka, Suzuki and Bocharov.

Claims	35 U.S.C. §	References/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
7, 8, 19	103	Peterka, Bocharov, Peterka308, Chen	7, 8, 19	
Overall Outcome			1–8, 10, 12, 14, 16–20	

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	1–8, 10, 12, 14, 16–20
Substitute Claims Proposed in the Amendment	21–37
Substitute Claims: Motion to Amend Granted	
Substitute Claims: Motion to Amend Denied	21–37
Substitute Claims: Not Reached	

VI. ORDER

In consideration of the foregoing, it is hereby

ORDERED that claims 1–8, 10, 12, 14, and 16–20 of U.S. Patent No. 9,313,178 B2 have been shown to be unpatentable under 35 U.S.C. § 103;

FURTHER ORDERED that Patent Owner’s Revised Motion to Amend (Paper 32) 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.

IPR2025-00003
Patent 9,313,178 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
Kayvan Noroozi
NOROOZI PC
peter@noroozipc.com
kayvan@noroozipc.com