

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

I. INTRODUCTION

Google LLC and Lenovo (United States) Inc., (“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”). Paper 3. Ericsson AB (“Patent Owner”) filed a Preliminary Response (“Prelim. Resp.”). Paper 9. With our authorization, Petitioner filed a Reply and Patent Owner filed a Sur-Reply directed to the claim requirement, “detecting content encryption key rotation boundaries.” Ex. 3002; Papers 10, 12.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted unless the information presented in the Petition and any preliminary response shows that “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

For the reasons explained below, we determine that Petitioner has established a reasonable likelihood that it would prevail with respect to at least one challenged claim. Accordingly, we institute an *inter partes* review as to the challenged claims and grounds raised in the Petition.

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, 2011.¹ Ex. 1001, codes (54), (22), (45), (63), (60).

The '178 patent is directed to managing key rotation (use of a series of 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.

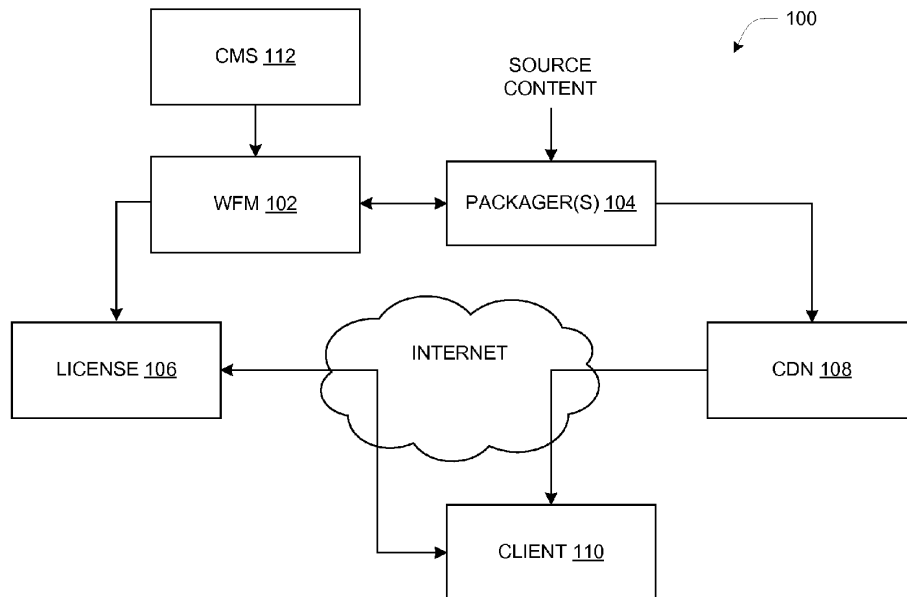


Fig. 1

¹ The effective priority date for the claims is not at issue here. Pet. 7.

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 an exemplary embodiment, each encryption key has a preset expiration time, measured by relative wall clock time, segment numbers, or number of video key frames. *Id.* at 6:13–25. However, 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.

Figure 3 is reproduced below.

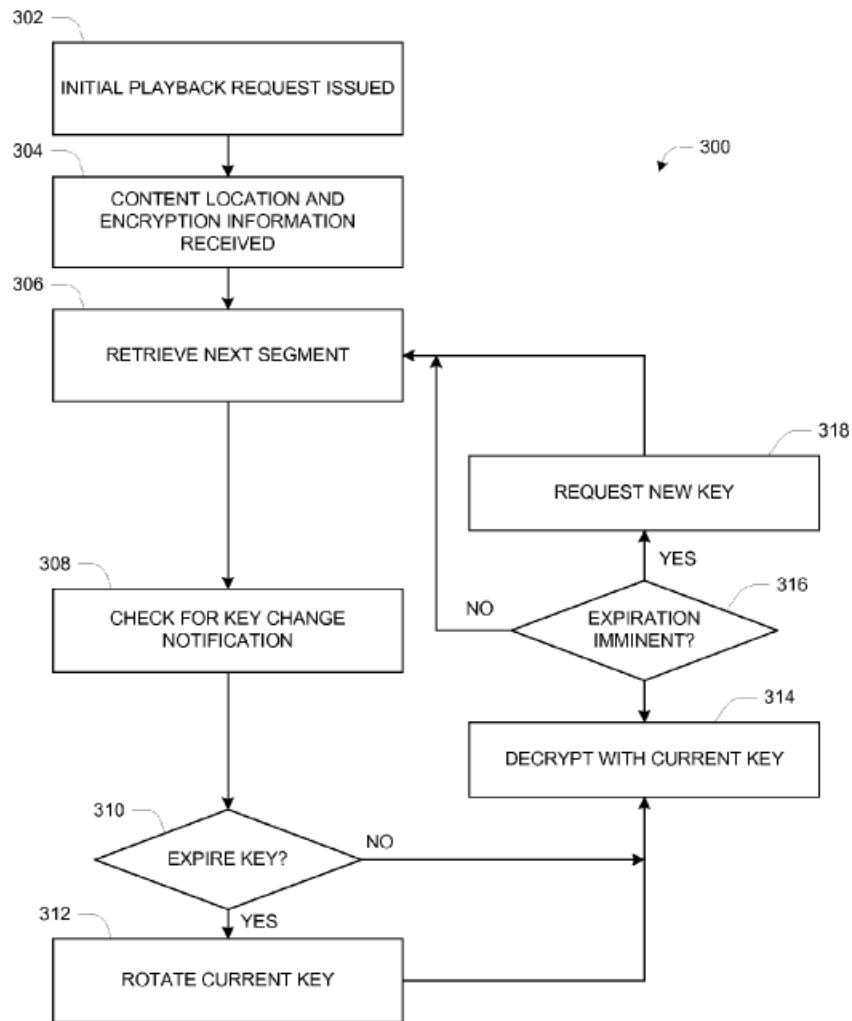


Fig. 3

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 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 ahead of time to prevent any latency in or interruption of decryption services. *Id.* at 11:38–45.

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;
 - 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. Asserted 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. §²	References
1–6, 10, 12, 16–18, 20	103	Peterka ³
1–6, 10, 12, 16–18, 20	103	Peterka, Suzuki ⁴
1–6, 10, 12, 14, 16–18, 20	103	Peterka, Bocharov ⁵
1–6, 10, 12, 14, 16–18, 20	103	Peterka, Suzuki, Bocharov
7, 8, 19	103	Peterka, Bocharov, Peterka308, ⁶ Chen ⁷

² 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.

³ Peterka, et al., US 2002/0172368 A1. Ex. 1005 (“Peterka”).

⁴ Suzuki, et al., 2004-166153. Ex. 1006 (“Suzuki”).

⁵ Bocharov, et al., US 2010/0235528 A1. Ex. 1007 (“Bocharov”).

⁶ Peterka, et al., US 2008/0270308 A1. Ex. 1008 (“Peterka308”).

⁷ Chen, et al., EP 1 418 756 A2. Ex. 1009 (“Chen”).

Petitioner also filed the Declaration of Anthony J. Wechselberger in support of the Petition. Ex. 1003.

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 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. Obviousness: Legal Standards

To prevail in its challenge, 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 non-obviousness (also called secondary considerations), such as commercial success, long-felt but unsolved needs, and failure of others.⁸ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We analyze grounds 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

⁸ No evidence of objective indicia of non-obviousness is of record.

(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 does not dispute the Petitioner's proposal at this time. Prelim. Resp. 8.

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-type 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) (2023). 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 believe the Board need resolve any claim construction issues at this stage..” Prelim. Resp. 8.

Nevertheless, the parties’ arguments with respect to claim 1 of the ’178 patent raise claim construction issues regarding the requirement of “detecting content encryption key rotation boundaries,” 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 directed to providing 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). A content distribution system is made up of servers that download streaming media to clients. *Id.* at Fig. 1, ¶ 38. In disclosed

embodiments, the content is divided into purchasable segments and encrypted with separate keys. *Id.* ¶ 99.

Figure 7A is reproduced below.

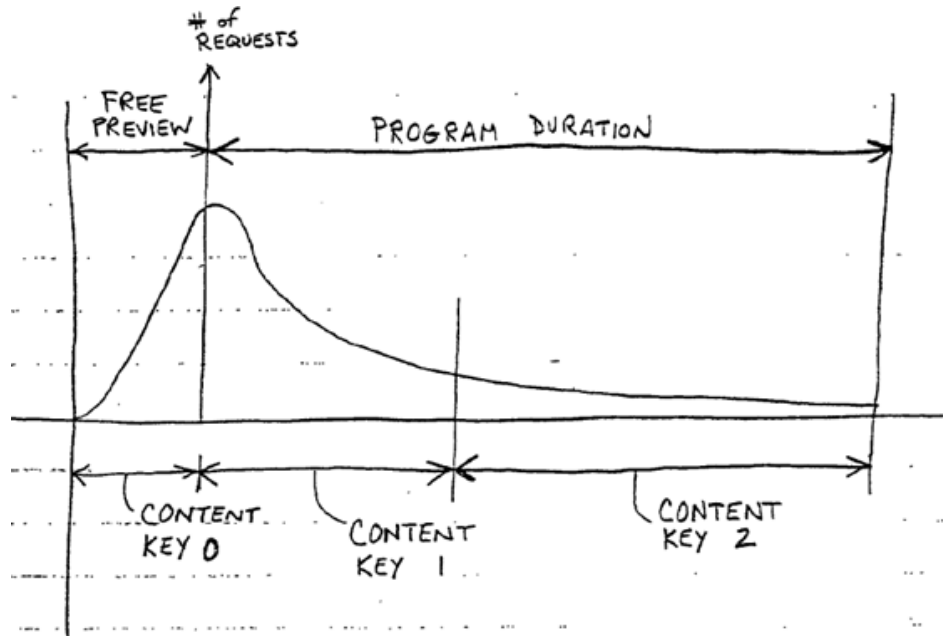


Figure 7A is a graph showing distribution of cryptographic keys during portions of a program. Ex. 1005 ¶ 21. During the “Free Preview” period, the content is encrypted with “Content Key 0,” which is freely distributed. *Id.* ¶¶ 91–92. Subsequent keys are required to decrypt the remainder of the program content, delivered only to those clients that purchased the content. *Id.* ¶¶ 92–93.

Disclosed embodiments 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.” *Id.* ¶ 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”), ¶ 105 (“Under the pull model, each client keeps track of the keys and their

expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions”), ¶ 106 (“[T]he 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”).

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).⁹

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).

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

⁹ Based on the present record, we make no determination at this stage of the proceeding that the preamble of claim 1 (or of claim 16) is limiting.

clients to extract the content. Pet. 22 (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 23–28 (citing Ex. 1005, Figs. 7B, 8, ¶¶ 94–106, 121; Ex. 1003 ¶¶ 86–101). As to the required encryption key and expiration time items, we note that Peterka explicitly discloses that the messages contain encryption keys and “the time remaining in the lifetime of the key.” Ex. 1005 ¶ 121. For the encryption key identifier requirement, Petitioner relies on additional items contained in the messages: the “type of key,” a “parity” value, “a sequence number or a time stamp,” and a “keyed message authentication code (MAC), or a public key digital signature for authentication,” 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 ¶¶ 91–96).

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 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).

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).

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’s response relies on its construction of the claim 1 requirement, “detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content” (hereafter, the “detecting requirement”), asserting that the requirement “does not refer to all key rotation boundaries because not all key rotation boundaries require or entail the step of ‘detecting’ as recited in the claims.” Prelim. Resp. 21. Patent Owner argues that this requirement “is thus not met by merely ‘monitoring’ or ‘checking’ for key rotation boundaries, such as by monitoring or checking a timer” — and therefore Petitioner’s reliance on the “pull” embodiment of Peterka does not satisfy this requirement. *Id.* at 9–10.

Patent Owner argues that “checking” and “detecting” are two separate steps: first “the client 110 **checks** to see if a key change is signaled, i.e., a key change was requested outside of any fixed duration lifespan,” and **subsequently** “[i]f a content encryption key change request is **detected**, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used.” Prelim. Resp. 10 (citing Ex. 1001, 10:39–42, 10:65–11:1). Therefore, argues Patent Owner, “[t]he patent thus teaches that “checking” for a key change notification signal is a separate and preceding step to “detecting” such a notification, and thus a key rotation boundary.” *Id.* at 10–11. And further, argues Patent Owner, “[i]t is the separate step of ‘detecting’ the key change

notification — not the mere act of ‘checking’ — that is recited by the claims.” *Id.* at 11.

Patent Owner cites examples demonstrating that the ’178 patent maintains the distinction between “checking” and “detecting” throughout the Specification (Prelim. Resp. 11–12):

“In step 316, the client ***checks*** to see if the current content encryption key is going to ***expire*** in the near future or if a content encryption key change request for a future segment was ***detected*** in step 308.” Ex. 1001, 11:38–41 (emphasis added).

“If the current content encryption key is not close to expiring ***and*** a content encryption key change request was ***not detected*** in step 308, processing proceeds back to step 306” Ex. 1001, 11:45–48 (emphasis added).

“[i]f the current content encryption key is within a fixed threshold of expiring ***or*** a content encryption key change request was ***detected*** in step 308, processing proceeds to step 318 where the client 110 requests a new content encryption key from the license server 106.” Ex. 1001, 11:48–53 (emphasis added).

In sum, argues Patent Owner:

Critically, in no instance does the ’178 Patent use the term “detect” to describe a key change boundary associated with the expiration of a timer. And in no instance does the ’178 Patent teach that merely checking for a non-timer-based key change notification is equivalent to actually detecting such a key rotation boundary.

Prelim. Resp. 13. Patent Owner argues that this distinction is supported by the fact that the server distributes the key lifespans to the clients, requiring only checking for the normal key expirations, whereas the key change notifications are embedded in headers or manifest files, and thus must be detected. *Id.* at 13–16 (citing Ex. 1001, 3:46–47, 10:39–48, 10:50–11:1,

11:38–41, 11:45–53). Patent Owner argues that this dovetails with the dictionary definitions of “checking” (“to make certain that something or someone is correct, safe, or suitable by examining it, him, or her quickly,” or “to find out about something”) versus “detecting,” (“to notice something that is partly hidden or not clear, or to discover something, especially using a special method,” or “to discover something, usually using special equipment”). *Id.* at 16 (citing Exs. 2002, 2003). Patent Owner asserts that checking a timer requires only a quick examination whereas a key change notification is “not clear and is at least partially hidden,” thus requiring detecting rather than mere checking. *Id.* at 16–17. Patent Owner also cites court decisions (in unrelated cases) that drew a distinction between “detect” and other terms. *Id.* at 17–19.

Patent Owner also argues that Petitioner’s alternative reliance on the disclosure in Peterka of methods for sending signals to the client for detection of encryption key rotation boundaries (Pet. 33–34) is unsound, because that portion of Peterka relates to the “Push” embodiment rather than the “Pull” embodiment, and the former embodiment sends keys to the client without any request from the client, inconsistent with the requirements of the claims. Prelim. Resp. 22–25 (citing Ex. 1005 ¶¶ 116–117).

Patent Owner makes the same arguments discussed above for the corresponding requirement of independent claim 16. Prelim. Resp. 20–21. Patent Owner does not specifically respond to any of Petitioner’s arguments regarding the other requirements of claims 1 or 16. *See generally* Prelim. Resp. Nonetheless the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

c) Petitioner's Reply and Patent Owner's Sur-Reply

Petitioner points out that the '178 patent, in describing the Figure 3 flow diagram that depicts the key change operations caused by both timer expirations and key change requests, states, "FIG. 3 is a flow chart 300 describing a process for **detecting** the rotation of content encryption keys and retrieving updated content encryption keys." Reply 1–2 (citing Ex. 1001, 9:47–49) (emphasis added). Petitioner further cites the Figure 3 description for step 110 stating that:

[T]he client 110 **checks** the expiration of current content key to see if a new key should be applied. There are two cases-normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted.

Reply 2 (citing Ex. 1001, 11:2–7) (emphasis added). Thus, argues Petitioner, the word choice of "detecting" in claim 1 does not distinguish between these two ways that key change boundaries occur. *Id.*

Petitioner argues that Patent Owner's assertion that "detecting" a key change notification is a "further distinct step" from checking for that notification, based on the fact that the notification is "**partly hidden or not clear,**" contradicts arguments that it successfully made in the related ITC proceeding (Inv. No. 337-TA-1376). Reply 2–3 (citing Ex. 1033, 14; Ex. 1036, 52, 54, 56; Ex. 1037, 3) (emphasis in original). Petitioner argues that there is no language in the '178 patent, file history, or ordinary meaning of the word that narrows "detecting" to hidden or unclear information. *Id.* at 3–4.

In regard to its alternative reliance on Peterka's use of signals to detect content encryption key rotation boundaries, Petitioner disputes Patent

Owner’s assertion that this disclosure only related to push rather than pull embodiments, citing its expert’s testimony, and contradictory positions taken in the ITC proceeding. Reply 5 (citing Ex. 1003 ¶¶ 49, 115–117; Ex. 1005 ¶ 121; Ex. 1036, 56, 59).

In its Sur-Reply, Patent Owner repeats its arguments to the effect that the ’178 patent does draw a distinction between “checking” and “detecting,” given such disclosures as “the client 110 *checks* to see . . . if a content encryption key change request for a future segment *was detected*.” Sur-Reply 1 (citing Ex. 1001, 11:38–41). Patent Owner disputes Petitioner’s assertion that Patent Owner relies on attorney argument and “cherry-picking” from dictionary definitions. *Id.* at 2–4. Patent Owner also disputes that it took contradictory positions in the ITC proceeding. *Id.* at 3–4.

In regard to Petitioner’s alternative reliance on Peterka’s signaling, Patent Owner argues that the disclosed signaling only pertains to keys that already have been provided to the client, which is inconsistent with the claim requirement that the client request a new key. Sur-Reply 5.

d) Analysis

We are not persuaded at this stage by Patent Owner’s interpretation of the detecting requirement. As discussed above, that interpretation hinges on the assumption that “detecting” in the claim limitation at issue only refers to detecting rotation boundaries that occur between normal rotation boundaries — *i.e.*, key rotations triggered by security issues or other specific events, rather than normal key rotations due to expiration of the current key.

This construction, however, improperly limits the scope of the claim to one aspect of the disclosed embodiment of the ’178 patent that deals with

the special case of key changes requested for security reasons outside of any fixed duration lifespan. Ex. 1001, 10:40–42. Considering, as we must, the disclosure of the ’178 patent as a whole, the scope of the disclosure is directed broadly to key rotation in general, whether due to scheduled key expiration times or otherwise. *Id.* at code (57), Fig. 3, 1:63–65, 2:23–25, 3:26–28, 9:47–49; *see also Superguide Corp. v. DirecTV Enter., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (“Though understanding the claim language may be aided by explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim. For example, a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment”).

There is only one specific mention of the detecting requirement in the ’178 specification: “the client device ***detects*** content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content.” Ex. 1001, 2:23–25 (emphasis added). This appears to broadly refer to any encryption key boundary, no matter the cause — there is no other specific reference to the detection requirement in the specification that would justify narrowing the scope of this requirement in the manner that Patent Owner proposes.

Moreover, the ’178 patent, in describing the Figure 3 flow diagram that depicts the key change operations due to both timer expirations and key change requests, broadly states, “FIG. 3 is a flow chart 300 describing a process for ***detecting*** the rotation of content encryption keys and retrieving updated content encryption keys.” *Id.* at 9:47–49 (emphasis added). Again, given that Figure 3 describes both causes of key rotations,

this introductory sentence uses “detecting” to broadly encompass the occurrence of any encryption key rotation boundary, no matter the cause.

Later in the description of Figure 3, Step 310, labeled “Expire Key?” is explained:

In step 310, the client 110 *checks* the expiration of current content key to see if a new key should be applied. There are two cases — normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted.

Ex. 1001, 11:3–8 (emphasis added). Here, the word “checks” is used instead of “detects,” nevertheless applying to key change operations due to both timer expirations and key change requests. From this we preliminarily conclude that the ’178 patent uses the words “checks” and “detects” interchangeably without any implication that the former refers to timer expirations and the latter to key change notifications.

Patent Owner, arguing otherwise, relies on yet a different portion of the Figure 3 description that explains step 316, labeled “Expiration Imminent?”:

In step 316, the client 110 *checks* to see if the current content encryption key is going to expire in the near future or if a content encryption key change request for a future segment was *detected* in step 308.

Ex. 1001, 11:38–41 (emphasis supplied). We do not accord the positioning of the words “checks” and “detected” in this sentence the significance that Patent Owner asserts. “Checks” applies to both causes of key rotation, and “detected” only refers to a different step that *precedes* the step of detecting/checking a key rotation boundary. Moreover, step 308 of Figure 3, referred to in above-quoted passage in the context of “detected,” is labeled in

the figure, “**Check** For Key Change Notification” (emphasis added), further confirming the interchangeable usage of “check” and “detect” by the ’178 patent.

Patent Owner’s reliance on dictionary definitions of “check” and “detect” is unavailing — granted, the words are not synonymous, but “check” in the sense of “check something for something” and “detect” in the sense of “to discover something” support our conclusion of their interchangeability in this context. Exs. 2002, 2003. The claim was drafted to state “**detecting** content encryption key rotation boundaries,” but could just as well have stated, “**checking** for content encryption key rotation boundaries.”

In sum, we conclude at this stage that the “detecting” limitation refers to all boundaries between key rotations, whether caused by normal expiration of a key or by forced rotation due to security issues. The “detecting” part of the limitation refers to detecting any key rotation boundary. Thus, we determine that Petitioner’s reliance on the disclosure in Peterka of 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,” is reasonably likely to meet the detecting requirement of claims 1 and 16.¹⁰

Based on this, and on our further review of Petitioner’s reliance on Peterka’s disclosures in challenging the remaining requirements of claims 1 and 16, we determine for purposes of this Decision that the information

¹⁰ We discuss Petitioner’s alternative reliance on the disclosure in Peterka of using a predetermined bit to signal encryption key rotation boundaries in connection with claim 12 below.

presented in the record demonstrates a reasonable likelihood that Petitioner will prevail in establishing that independent claims 1 and 16 are unpatentable under 35 U.S.C. § 103 over Peterka.

3. Claims 2–6, 10, 17, and 18

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 that “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).

Patent Owner does not specifically respond to any of Petitioner’s arguments regarding dependent claims 2–6, 10, 17, and 18. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. We determine, on the current record and for purposes of this Decision, that the information presented in the Petition demonstrates a reasonable likelihood that Petitioner will prevail in establishing that claims 2–6, 10, 17, and 18 are unpatentable under 35 U.S.C. § 103 over Peterka.

4. *Claims 12 and 20*

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).

This argument by Petitioner depends on Petitioner's alternative argument regarding the detecting requirement of claim 1, relying 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. Pet. 33–34. As discussed above, the parties dispute whether this signalling capability only pertains to the “Push” embodiment of Peterka, and is therefore incompatible with the requirement of the claims that sending keys to the client must be preceded by a request for keys from the client. Prelim. Resp. 22–25; Reply 5; Sur-Reply 5.

At this stage, after reviewing the current record, we determine that Petitioner demonstrates a reasonable likelihood that it will prevail in establishing that claims 12 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. 66–68.¹¹

¹¹ 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. 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 at this stage, 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.

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 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.* at ¶¶ 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 does not specifically address the merits of combining Peterka, Suzuki, and Bocharov. *See generally* Prelim. Resp. Nonetheless the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). For purposes of this Decision, we determine that Petitioner has provided sufficiently articulated reasoning with rational underpinnings for the proffered combined teachings of Peterka, Suzuki, and Bocharov.

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 requirement 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).

Other than the arguments discussed above in connection with the challenges to claims 1, 12, 16, and 20 based on Peterka alone, Patent Owner does not specifically respond to any of Petitioner’s other arguments regarding claims 1–6, 10, 12, 14, 16–18, and 20. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. We determine, on the current record and for purposes of this Decision, that the information presented in the Petition demonstrates a reasonable likelihood that Petitioner will prevail in establishing that claims 1–6, 10, 12, 14, 16–18, and 20 are unpatentable under 35 U.S.C. § 103 over the combination 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* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

For purposes of this Decision, we determine that Petitioner has provided sufficiently articulated reasoning with rational underpinnings for the proffered combined teachings of Peterka, Bocharov, Peterka308, and Chen.

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).

Patent Owner does not specifically respond to any of Petitioner’s arguments regarding dependent claims 7, 8, and 19. *See generally* Prelim. Resp. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378. We determine, on the current record and for purposes of this Decision, that the information presented in the Petition demonstrates a reasonable likelihood that Petitioner will prevail in establishing 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. CONCLUSION

After considering the evidence and arguments presented in the Petition and the Preliminary Response, Petitioner has established a reasonable likelihood of prevailing on its assertion that at least one claim of

the '178 patent is unpatentable. Accordingly, we institute an *inter partes* review on all the challenged claims and all of the grounds presented in the Petition. At this stage of the proceeding, we have not made a final determination as to the patentability of these challenged claims.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that pursuant to 35 U.S.C. § 314, *inter partes* review is instituted as to the challenged claims of the '178 patent with respect to all grounds of unpatentability presented in the Petition; and

FURTHER ORDERED that *inter partes* review is commenced on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

IPR2025-00003
Patent 9,313,178 B2

PETITIONER:

Scott McKeown
Anant Saraswat
smckeown-ptab@wolfgreenfield.com
asaraswat-ptab@wolfgreenfield.com

PATENT OWNER:

Peter Knops
Kayvan Noroozi
peter@noroozipc.com
kayvan@noroozipc.com