Trials@uspto.gov
571-272-7822

Paper 11
Entered: September 1, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner.

IPR2022-00618
Patent 9,313,178 B2

Before GEORGIANNA W. BRADEN, NATHAN A. ENGELS, and NORMAN H. BEAMER, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

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

Google Exhibit 1028
Google v. Ericsson

I. INTRODUCTION

On February 25, 2022, Apple Inc. ("Petitioner") filed a Petition ("Pet.") pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–20 of U.S. Patent No. 9,313,178 B2 ("the '178 patent"). Paper 2. On July 8, 2022, Telefonaktiebolaget LM Ericsson ("Patent Owner") filed a Preliminary Response ("Prelim. Resp."). Paper 9.

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).

[1] The effective priority date for the claims is not at issue here.

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.

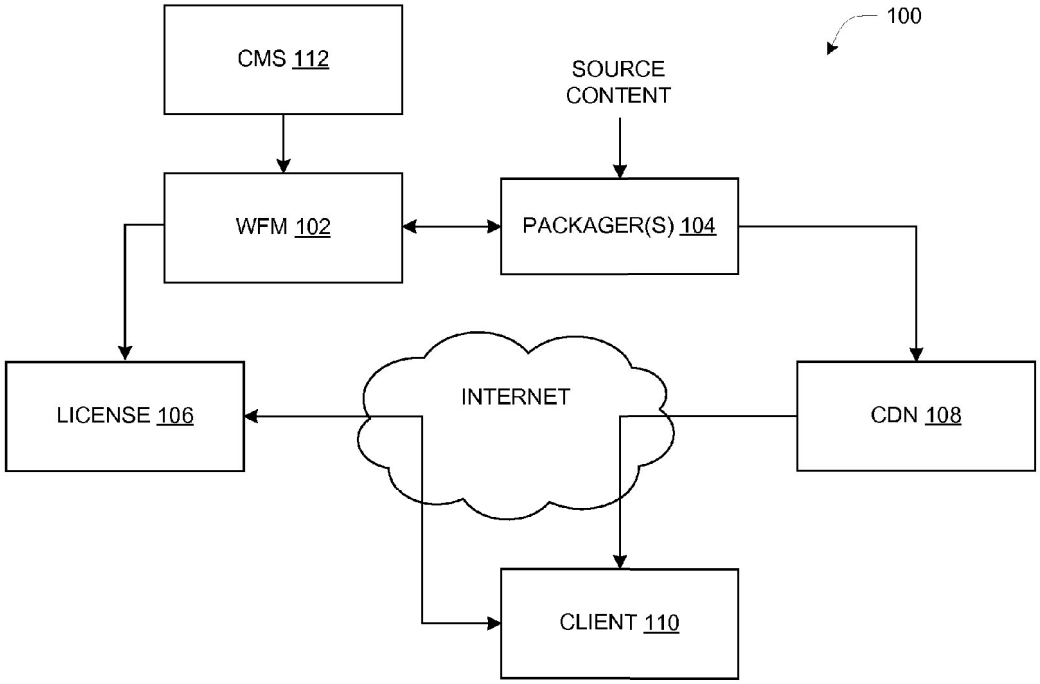

Fig. 1

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 clients 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.

Figure 3 is reproduced below.

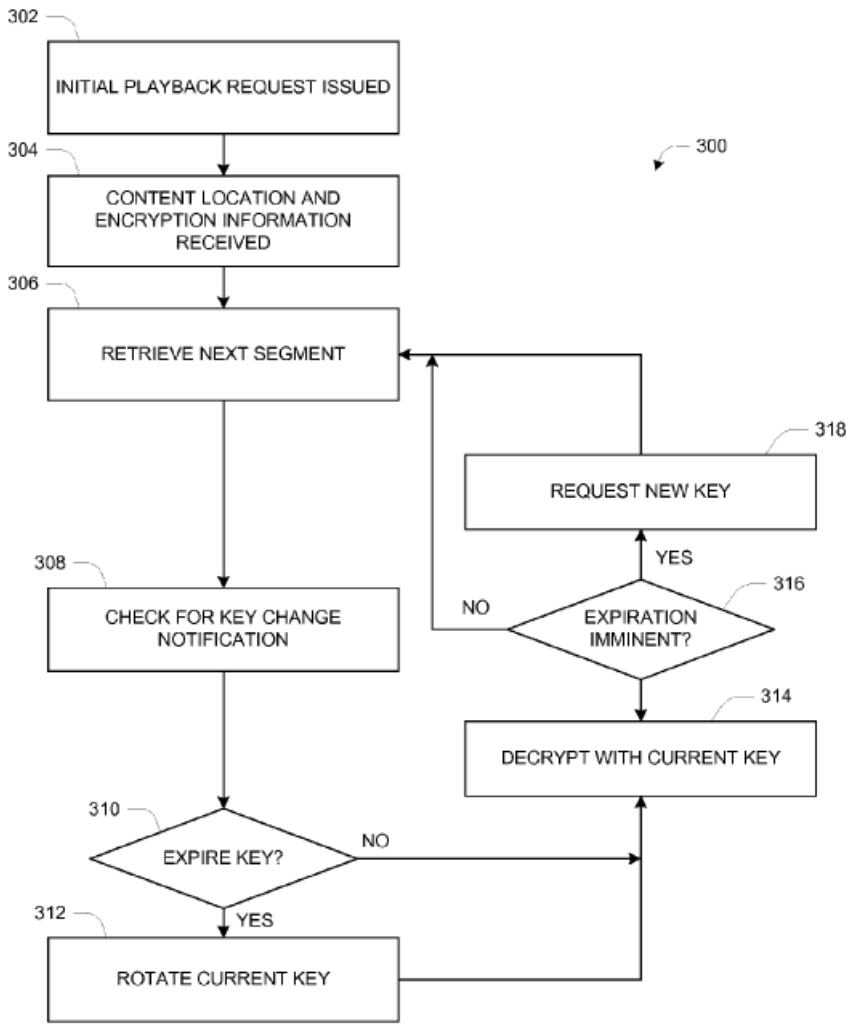

Fig. 3

Figure 3 is a flow diagram showing content downloading and decryption using content encryption key rotation. Ex. 1001, 4:42–43. 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 detect 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.* at 10:40–43, 10:65–11:2.

B. Illustrative Claim

Independent claim 1 is reproduced below.

> 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.

C. References

Petitioner relies on the following references (Pet. ii, 1):

- Peterka, US 2002/0172368 A1. Ex. 1004 ("Peterka").
- Bocharov, et al., US 2010/0235528 A1. Ex. 1005 ("Bocharov").
- Chen, et al., EPU 1 418 756 A2. Ex. 1006 ("Chen").
- Balraj, et al., US 2009/0254708 A1. Ex. 1007 ("Balraj").
- Peterka, et al., US 2008/0270308 A1. Ex. 1009 ("Peterka308").
- Kelly, et al., US 2005/0138362 A1. Ex. 1010 ("Kelly").
- Eisen, et al., US 2011/0067012 A1. Ex. 1011 ("Eisen").

Petitioner also filed the Declaration of Dr. Aviel Rubin in support of the Petition. Ex. 1003 ("Rubin Decl.").

D. Asserted Challenges to Patentability

Petitioner challenges the patentability of claims 1–20 of the '178 patent on the following basis (Pet. 1):

Claims Challenged	35 U.S.C. §[2]	References
1–4, 6–7, 12–13, 16–20	103	Peterka, Bocharov
7–9, 14–15, 19	103	Peterka, Bocharov, Peterka308, Chen
5	103	Peterka, Bocharov, Balraj
10	103	Peterka, Bocharov, Kelly
11	103	Peterka, Bocharov, Kelly, Eisen

[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 that became effective after the original filing of the application for the '178 patent. Therefore, we apply the pre-AIA versions of these sections.

E. Real Parties in Interest

Petitioner identifies itself as the real party in interest. Pet. 66. Patent Owner identifies Ericsson AB and Ericsson Inc. as the real parties in interest. Paper 6 (Patent Owner's Mandatory Disclosures), 1.

F. Related Proceedings

The parties do not identify any related matters. Pet. 66; Paper 6, 1.

III. ANALYSIS

A. Obviousness: Legal Standards

A claim is unpatentable for obviousness if, to one of ordinary skill in the pertinent art, "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103). The question of obviousness is resolved on the basis of underlying factual determinations, including "the scope and content of the prior art"; "differences between the prior art and the claims at issue"; and "the level of ordinary skill in the pertinent art." *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, objective indicia of non-obviousness, such as "commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or

nonobviousness, these inquiries may have relevancy."[3] *Graham*, 383 U.S. at 17–18.

A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. Rather, an obviousness determination requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citation omitted); *see KSR*, 550 U.S. at 418 (for an obviousness analysis, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements [in the way the claimed] new invention does"). "Although the *KSR* test is flexible, the Board 'must still be careful not to allow hindsight reconstruction of references . . . without any explanation as to *how* or *why* the references would be combined to produce the claimed invention.'" *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016) (citation omitted).

Furthermore, an assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *accord In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (stating that "'conclusory statements'" amount to an "insufficient

[3] At this stage, no issues of objective indicia of non-obviousness are presented.

articulation [] of motivation to combine"; "instead, the finding must be supported by a 'reasoned explanation'" (citation omitted)); *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) ("To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.").

A reason to combine must be "accompanied by a reasonable expectation of achieving what is claimed in the patent-at-issue." *Intelligent Bio-Sys*, 821 F.3d at 1367. "The reasonable expectation of success requirement refers to the likelihood of success in combining references to meet the limitations of the claimed invention." *Id.*

B. Level of Skill in the Art

Petitioner asserts:

> [A] person of ordinary skill in the art at the time of the alleged invention ("POSITA") would have had a Bachelor's degree in computer science, computer engineering, or a related field, and 2-3 years of practical engineering experience, including experience designing or researching 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.

Pet. 5 (citing Rubin Decl. ¶¶ 23–26).

Patent Owner does not dispute Petitioner's proposal at this stage of the proceeding. Prelim. Resp. 5.

Petitioner's proposal is consistent with the level of ordinary skill in the art reflected by the prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir.

1995). On this record, the level of ordinary skill is neither in dispute nor dispositive of any challenge. For purposes of this Decision, we apply Petitioner's articulation.

C. Claim Construction

The Petition was accorded a filing date of February 25, 2022. Paper 5, 1. In an *inter partes* review for a petition filed on or after November 13, 2018, a claim "shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." 37 C.F.R. § 42.100(b) (2019). We apply the claim construction standard from *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (*en banc*).

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 "no formal claim constructions are presently necessary." Pet. 5. Patent Owner states that it "does not believe the Board need resolve any claim construction issues at this stage." Prelim. Resp. 6.

However, Patent Owner's arguments with respect to claim 1 of the '178 patent do raise claim construction issues, which we discuss in Section III.D.4.b) below.

D. Alleged Obviousness of Claims 1–4, 6–7, 12–13, and 16–20 over Peterka and Bocharov

Petitioner challenges claims 1–4, 6–7, 12–13, and 16–20 as obvious over the combination of Peterka and Bocharov. Pet. 12–44.

1. Peterka

Peterka, titled "Intial [sic] Free Preview For Multimedia Multicast Content," was filed October 26, 2001, and published November 21, 2002. Ex. 1004, 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. 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.

Figure 7A is reproduced below.

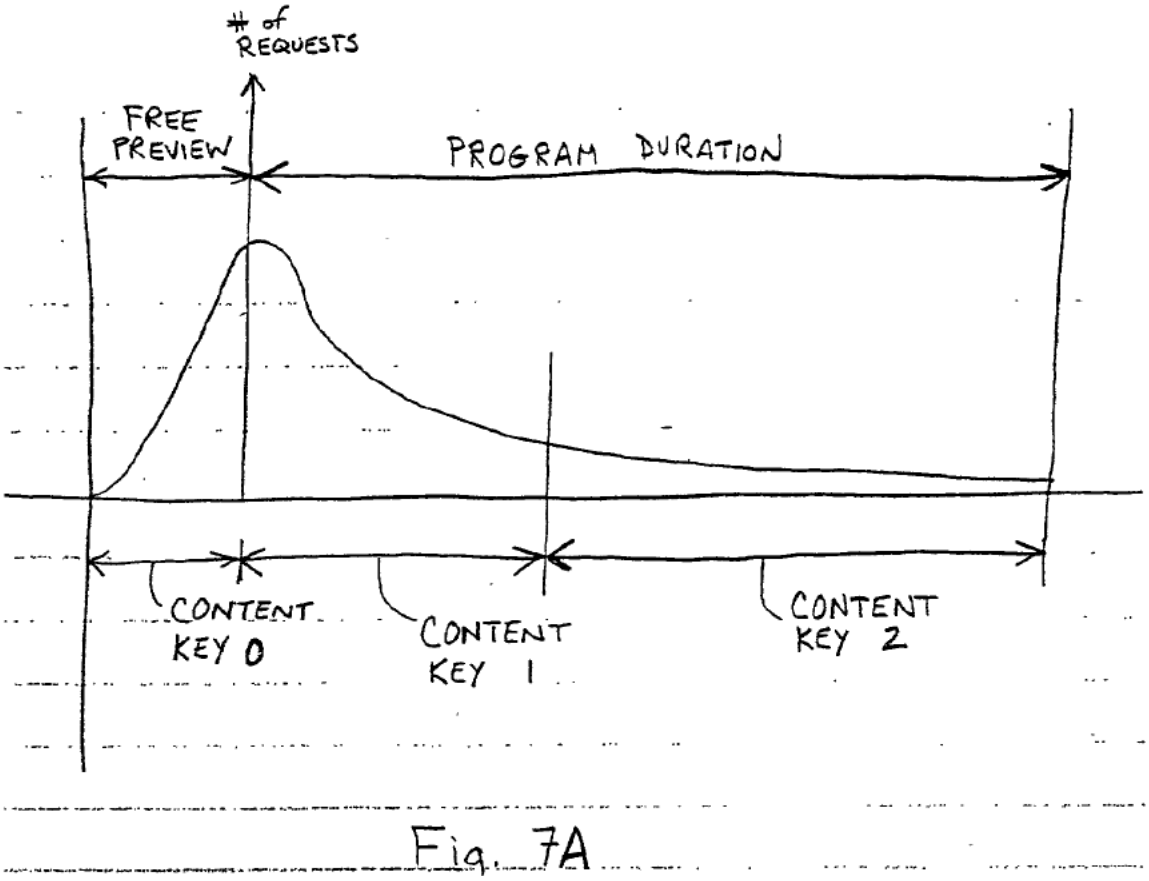

Figure 7A is a graph showing distribution of cryptographic keys during portions of a program. Ex. 1004 ¶ 21. During the "Free Preview" period, the content is encrypted with "Content Key 0," which is freely distributed. *Id.* ¶¶ 91–92. Subsequent keys are required to decrypt the remainder of the program content, delivered only to those clients that purchased the content. *Id.* ¶¶ 92–93.

2. Bocharov

Bocharov, titled "Delivering Cacheable Streaming Media Presentations," was filed March 6, 209, and published September 16, 2010. Ex. 1005, codes (54), (22), (43). 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 and Bocharov

Petitioner argues that one of ordinary skill would have had reason to combine the teachings of Peterka and Bocharov, resulting in a combination that would have rendered obvious, for example, independent claim 1. Pet. 12–18. Petitioner argues that Peterka indicates that video content can be streamed using various protocols and bit rates, but does not provide implementation details. *Id.* at 13 (citing Rubin Decl. ¶ 69). However, argues Petitioner, one of ordinary skill in the art would have had reason to use manifest files to provide the necessary information to handle different protocols and bit rates, because that technique was well known as evidenced by the teachings of Bocharov. *Id.* at 13–18 (citing Rubin Decl. ¶¶ 70–75). Petitioner argues that one of ordinary skill in the art would have been so motivated because both Peterka and Bocharov are directed to highly similar systems for live streaming of media content, and provide solutions for managing heavy loads resulting from many users. *Id.*

Patent Owner does not specifically address the merits of combining Peterka 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 and Bocharov.

4. 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. 18 (citing Ex. 1004, Figs. 1, 3, ¶¶ 12, 83, 94; Rubin Decl. ¶¶ 76–77).[4]

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. 19–21 (citing Ex. 1004, Figs. 7A, 7B, 8, 18–20, ¶¶ 38, 55–56, 91, 101, 104–106, 110, 121–125, 131, 137; Rubin Decl. ¶¶ 78–81).

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 Dr. Rubin, one of ordinary skill would have known would have been parsed by clients to extract the content. Pet. 22–23 (citing Ex. 1004, Fig. 7B, ¶¶ 104, 121–125; Rubin Decl. ¶¶ 82–91). In particular, Petitioner argues that the messages include the required content encryption keys,

[4] Based on the present record, we make no determination at this stage of the proceeding that the preamble of claim 1 is limiting.

content encryption key identifiers, and content encryption key expiration times. *Id.* at 23–26 (citing Ex. 1004, ¶¶ 105–106, 114, 117–121; Rubin Decl. ¶¶ 83–86). 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. 1004 ¶ 1121. 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. 24–26 (citing Rubin Decl. ¶ 85).

For the claim 1 requirement, "retrieving content and manifest files from a content delivery server," Petitioner relies on the disclosures in Peterka and Bocharov of clients receiving content from servers, and in addition the disclosures in Bocharov of receiving manifest files from a sever, and, as discussed above, argues that it would have been obvious to combine the teachings of Peterka and Bocharov such that the client device would retrieve content and manifest files from a content delivery server. Pet. 32–34 (citing Ex. 1004, Fig. 1, ¶¶ 38, 39, 40, 60, 71, 83, 135; Ex. 1005, Fig. 5, ¶¶ 7, 15, 22–25, 30–35, 49–53; Rubin Decl. ¶¶ 92–94).

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 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. 34 (citing Ex. 1004 ¶¶ 116–121; Rubin Decl. ¶ 95). Petitioner also relies 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." *Id.* at 34–35 (citing Ex. 1004 ¶¶ 105–106, 114; Rubin Decl. ¶¶ 96–97).

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 a "pull model." Pet. 35–36 (citing Ex. 1004, Fig. 8, ¶¶ 82, 105–106, 114; Rubin Decl. ¶ 98).

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. 1004 ¶¶ 90, 92, 108, 116; Rubin Decl. ¶¶ 101–102).

Independent claim 16 is a device counterpart to method claim 1, and Petitioner's arguments and reliance on the combination of Peterka and Bocharov for this claim are in substance the same as for claim 1. Pet. 43–44.

b) Patent Owner's Response

Patent Owner's response primarily 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 is limited to "the scenario in which the client receives a notification instructing it to rotate a key ***before*** the normal period-based expiration (i.e., "between periods of use") associated with that key." Prelim. Resp. 12. Patent Owner argues that this requirement is not met by detecting "the normal period-based expiration of the current key while decrypting content." *Id.* at 15.

Patent Owner's interpretation of the detecting requirement is premised on a specific grammatical construction of the wording of the requirement in which "detecting" refers to detecting rotation boundaries that occur between normal key expiration boundaries:

> [The limitation] requires "***detecting*** content encryption key rotation boundaries ***between periods of use*** of different content encryption keys in decrypting retrieved content." The terms "detecting" and "between periods of use of different content encryption keys" refer to the scenario in which the client receives a notification instructing it to rotate a key ***before*** the normal period-based expiration (i.e., "between periods of use") associated with that key.

Prelim. Resp. 12. Patent Owner points to the above-discussed provision in the '178 patent, illustrated as step 308 of Figure 3, for providing a new content encryption key before normal expiration of the current encryption key when the current key is deemed to be no longer secure (*e.g.*, if the content encryption key has been compromised), and to detect such a premature key change. Prelim. Resp. 8–11; Ex. 1001, Fig. 3 (step 308), 7:11–20, 10:39–43, 10:65–11:2. Patent Owner in particular relies on the statement in the '178 patent, when describing the process of changing the key outside of any fixed duration lifespan, that "[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." *Id.* at 12 (citing Ex. 1001, 10:65–11:1). Patent Owner argues that the occurrence of the word "detected" in this passage aligns with "***detecting*** content encryption key rotation boundaries" in the claim. *Id.* Patent Owner also relies on dependent claims 12–15, which specify various ways to detect key rotation boundaries, and which Patent Owner argues can only apply to the premature key changes, not to the normal period-based expiration of the current key. *Id.* at 13–15 (citing Ex. 1001, 12:65–13:13).

Patent Owner argues that, given this construction, Petitioner's reliance on the disclosure in Peterka of methods for signaling to the client information for the client to detect content encryption key rotation boundaries cannot satisfy the detecting requirement, because it only applies to the normal period-based expiration of the current key. Prelim. Resp. 17–19. Patent Owner also argues that 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," cannot satisfy the detecting requirement, because it also only applies to the normal period-based expiration of the current key. Prelim. Resp. 20–21.

Patent Owner also argues that the claim 1 limitation, "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," is not obvious in light of the combination of Peterka and Bocharov. Prelim. Resp. 19, 21–22. For Petitioner's reliance on the disclosure in Peterka of using a predetermined bit to signal encryption key rotation boundaries, Patent Owner argues that the new keys being signaled

are not received in response to request from the client for a new key. *Id.* at 19. Also, argues Patent Owner, neither the use of the predetermined bit, nor the "pull model" operations, satisfy the above discussed detecting requirement, which as discussed Patent Owner would limit to key changes ahead of the known expiry time of the current key. *Id.* at 21–22.

Patent Owner makes the same arguments discussed above for the corresponding requirements of independent claim 16. Prelim. Resp. 7, n. 1. 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) Analysis

We are not persuaded 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. Patent Owner's rationale for this construction is illustrated by the emphasis that Patent Owner applies when quoting the claim language:

> "***detecting*** content encryption key rotation boundaries ***between periods of use*** of different content encryption keys in decrypting retrieved content."

Prelim. Resp. 12.

However, this construction 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").

The basic error in Patent Owner's approach is revealed by its choice of emphasis in the above quotation of the claim limitation at issue — "***detecting***" and "***between periods of use***." Properly construed, it is the "***boundaries***" that are "***between periods of use*** of different content encryption keys," not the "detecting." In other words, the phrase "between periods of use . . ." modifies "boundaries," not "detecting."[5] 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. In terms of Figure 3 of the '178 patent, the detecting limitation corresponds to step 316, not step 308:

[5] *See The Chicago Manual of Style Online*, 17th Edition, § 5.178 ("Placement of prepositional phrases: A prepositional phrase with an adverbial or adjectival function should be as close as possible to the word it modifies to avoid awkwardness, ambiguity, or unintended meanings.")

> 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). As stated in this description of step 316, normal expiration key boundaries are "check[ed]" — *i.e.* "detected." We are not persuaded that the use of the word "checks" in this description, rather than "detects," is somehow a disavowal of the broader construction of the detecting requirement that we adopt.

Patent Owner is correct that the detecting requirement covers detecting key rotation boundaries that are triggered by security issues, and that dependent claims 12–15 refer to specific methods for detecting such key changes. But Patent Owner erroneously excludes from claim coverage the detection of rotation boundaries due to normal key expiration.

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 claim 1.[6] Based on this, and on our further review of Petitioner's reliance on the combination of Peterka and Bocharov in challenging the remaining requirements of claims 1 and 16, we determine

---

[6] We agree, however, with Patent Owner that Petitioner's alternative reliance on the disclosure in Peterka of using a predetermined bit to signal encryption key rotation boundaries, outside the context of the "pull model" embodiment, is not persuasive because the new keys being signaled are not received in response to request from the client for a new key. Prelim. Resp. 19. Patent Owner also discusses a "combination of the push and pull model" of Peterka, which was not raised by Petitioner, and which we do not need to consider. *Id.* at 22–24.

for purposes of this decision that the information presented in the Petition 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 the combination of Peterka and Bocharov.

5. Claims 2–4, 6–7, 12–13, and 17–20

a) Petitioner's Challenge

Claim 2 adds the requirement that the playback request response includes information about a future encryption key as well as the current key. Ex. 1001, 12:23–27. Claim 17 adds a commensurate limitation. *Id.* at 14:12–17. Petitioner relies on a statement in Peterka describing "a key management approach where each rabbit [sic] is given keys to the current as well as the next segment." Pet. 37, 44 (citing Ex. 1004 ¶ 80; Rubin Decl. ¶¶ 87–91, 103–104). Petitioner's expert Dr. Rubin acknowledges the unexplained use of the word "rabbit" in this statement, but opines that "in the context of Peterka's system in which keys are distributed to client devices, a [person of skill in the art] would have understood Peterka's "key management approach" as described in paragraph [0080] to involve each client being given keys to the current as well as the next segment." Rubin Decl. ¶ 87, n. 3.

Claim 3 requires the key expiration be expressed as "an expected minimum interval between periodic key rotation," and claim 4 further requires timing the prefetching based on an expected expiration of the current key. Ex. 1001, 12:28–36. Claim 18 adds a commensurate limitation. *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. 37–39, 44 (citing Ex. 1004 ¶¶ 78–82, 99–101, 105–106, 110, 121; Rubin Decl. ¶¶ 105–108). Petitioner's expert Dr. Rubin opines that, in view of these disclosures, it would have been obvious that key rotation would occur on a periodic basis that corresponds to the periodic distribution of new keys, that periodic key rotation would be a predictable option for dividing media streams into segments, and to express the key expiration time as recited in claim 3 to inform the client device of the period of key rotation so that the client could readily project key rotation boundaries and determine an appropriate time to request a new key ahead of the next boundary. Rubin Decl. ¶¶ 105–106. 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. 32–37, 44 (citing Ex. 1004, Fig. 8, ¶¶ 82, 105; Rubin Decl. ¶¶ 109–110).

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 disclosure in Peterka that clients keep track of the keys and their expiration times and actively request new keys before the current keys expire so as to avoid service interruptions, and argues that one of ordinary skill would have understood that a client device

would request a new content encryption key before the expected expiration of the content encryption key currently being applied, and therefore the client device would pre-fetch the next un-retrieved key within 100% (a "fixed percentage") of the fixed periodic content encryption key expiration interval. Pet. 40–41 (citing Ex. 1004 ¶¶ 82, 105, 106; Rubin Decl. ¶¶ 111–112).

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. *Id.* at 14:23–25. These claims are discussed below in connection with Ground 1B.

Claim 12 requires key boundary detection "based on real-time in-band notifications." Ex. 1001, 12:67–67. Claim 20 is commensurate. *Id.* at 14:26–28. Claim 13 further requires the key boundary detection to be "based on notifications in an unencrypted header portion of the encrypted content files." *Id.* at 13:1–3. For claim 12, Petitioner relies on the disclosure in Peterka of using a parity bit embedded directly in a packetized content stream to indicate if an old or current content key should be used as opposed to a new content key which has recently been distributed to the client. Pet. 42, 44 (citing Ex. 1004, Fig. 14, ¶¶ 116–121; Rubin Decl. ¶¶ 115–116). For claim 13, Petitioner further relies on the disclosure in Peterka of including the parity bit in the header of the packet. *Id.* at 42–43 (citing Ex. 1004 Fig. 14, ¶¶ 117–118, 120; Rubin Decl. ¶¶ 117–118).

b) Analysis

Patent Owner does not specifically respond to any of Petitioner's arguments regarding dependent claims 2–4, 6–7, 12–13, and 17–20. *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 2–4, 17, and 18 are unpatentable under 35 U.S.C. § 103 over the combination of Peterka and Bocharov. As mentioned above, we discuss claims 7 and 19 below in connection with Ground 1B.

However, for claim 6, we find that prefetching ***after*** expiration does not make sense in the context of the '178 patent. Nothing in the combination of Peterka and Bocharov would suggest prefetching after expiration, and therefore we are constrained to determine that the Petition does not demonstrate a reasonable likelihood that claim 6 is unpatentable under 35 U.S.C. § 103 over that combination. We note that Petitioner reserves the right to raise 35 U.S.C. § 112 defenses in other proceedings. Pet. 41, n. 2.

Also, for claims 12, 13, and 20, Petitioner relies on the embodiment disclosed in Peterka wherein a parity bit or other means is used to notify the client that a new encryption key has been sent. Pet. 34, 42–43. As discussed above for independent claim 1, Patent Owner argues, and we agree, that this embodiment does not teach or suggest the subject matter of claim 1 because the new keys being signaled are not received in response to request from the client for a new key. Prelim. Resp. 19. This flaw equally applies to Petitioner's arguments for dependent claims 12, 13, and 20. Therefore, we are not persuaded that the Petition demonstrates a reasonable likelihood that Petitioner will prevail in establishing that claims 12, 13, and 20 are

unpatentable under 35 U.S.C. § 103 over the combination of Peterka and Bocharov.

E. Alleged Obviousness of Claims 7–9, 14–15, and 19 over Peterka, Bocharov, Peterka308, and Chen

Petitioner challenges claims 7–9, 14–15, and 19 as obvious over the combination of Peterka, Bocharov, Peterka308, and Chen. Pet. 45–58.

Peterka308, titled "Method And Apparatus For Providing A Secure Trick Play," was filed August 27, 2007, and published October 30, 2008. Ex. 1009, 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. 1006, 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. 46–50 (citing Rubin Decl. ¶¶ 138–141). 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. Claim 9 additionally requires the identifier to be calculated as an expected wall clock time for applying the next content encryption key based on a fixed periodic content encryption key expiration interval. *Id.* at 12:55–58. For these claims, Petitioner relies on the timestamp disclosures of Peterka308 and the techniques for segmenting media content of Chen. Pet. 51–53, 58 (citing Ex. 1009 ¶¶ 24, 29; Ex. 1006, Figs. 2A–2C, ¶¶ 34–44; Rubin Decl. ¶¶ 142–147).

Patent Owner does not specifically respond to any of Petitioner's arguments regarding dependent claims 7–9 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 7–9 and 19 are unpatentable under 35

U.S.C. § 103 over the combined teachings of Peterka, Bocharov, Peterka308, and Chen.

Claims 14 and 15 depend from claim 12, as to which, as discussed above, we are not persuaded that the Petition demonstrates a reasonable likelihood of unpatentability under 35 U.S.C. § 103 over the combination of Peterka and Bocharov. Nothing that Petitioner has argued in regard to the further combination of Peterka, Bocharov, Peterka308, and Chen provides sufficient basis for altering our determination in regard to claim 12, and therefore, we are not persuaded that the Petition demonstrates a reasonable likelihood that Petitioner will prevail in establishing that dependent claims 14 and 15 are unpatentable under 35 U.S.C. § 103 over the combination of Peterka, Bocharov, Peterka308, and Chen.

F. Alleged Obviousness of Claim 5 Over Peterka, Bocharov, and Balraj

Petitioner challenges claim 5 as obvious over the combination of Peterka, Bocharov, and Balraj. Pet. 58–61.

Balraj, titled "Method And Apparatus For Delivering And Caching Multiple Pieces Of Content," was filed April 6, 2009, and published October 8, 2009. Ex. 1007, codes (54), (22), (43). Balraj is directed to secure content delivery, with the content divided into "epochs," including defining a service license prefetch time, which is the earliest time at which a content server can request encrypted presentation keys for an epoch. *Id.* at code (57), Figs. 4, 5, ¶ 61.

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 relies on the disclosure in Peterka of the pull key distribution model, in combination with the service license prefetch time of Balraj, arguing that "it would have been obvious for clients to prefetch the next un-retrieved content key (and any other necessary secondary keys) at the earliest prefetch time (i.e., a 'fixed duration before the expected expiration of the content encryption key currently being used') in order to maximize the time available for the server to return the next segment's keys." Pet. 59–61 (citing Ex. 1004 ¶¶ 104–106; Ex. 1007, Fig. 5, ¶¶ 61–66; Rubin Decl. ¶¶ 160–163).

Patent Owner does not specifically respond to any of Petitioner's arguments regarding dependent claim 6. *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 claim 5 is unpatentable under 35 U.S.C. § 103 over the combination of Peterka, Bocharov, and Balraj.

G. Alleged Obviousness of Claim 10 Over Peterka, Bocharov, and Kelly, and of Claim 11 Over Peterka, Bocharov, Kelly, and Eisen

Petitioner challenges claim 10 over the combination of Peterka, Bocharov, and Kelly, and of claim 11 over the combination of Peterka, Bocharov, Kelly, and Eisen. Pet. 61–66.

Kelly, titled "Authentication System For Networked Computer Applications," was filed December 22, 2004, and published June 23, 2003. Ex. 1009, codes (54), (22), (43). Kelly is directed, *inter alia*, to controlling server access using encrypted authentication tokens. *Id.* at ¶ 30.

Eisen, titled "System And Method For Generating White-Box Implementations Of Software Applications," was filed May 25, 2009, and published March 17,2011. Ex. 1011, codes (54), (22), (43). Eisen is directed, *inter alia*, digital rights management using white-box cryptography. *Id.* at code (57).

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 authentication token techniques of Kelly. Pet. 62–64 (citing Ex. 1004 ¶¶ 66, 75, 95, 136, 142–144, 146; Ex. 1010 ¶¶ 28–30, 42–43, 64–66; Rubin Decl. ¶¶ 165–168).

Claim 11 adds to claim 10 the requirement that "the token-based technique employs white box encryption to encrypt the token." Ex. 1001, 12:63–64. Petitioner relies on the disclosure in Eisen of white box encryption. Pet. 59–61 (citing Ex. 1011 ¶¶ 8–9, 26–36; Rubin Decl. ¶¶ 170–171).

Patent Owner does not specifically respond to any of Petitioner's arguments regarding dependent claims 10 and 11. *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 claim 10 is unpatentable under 35 U.S.C. § 103 over the combination of Peterka, Bocharov, and Kelly, and that Claim

11 is unpatentable under 35 U.S.C. § 103 over the combination of Peterka, Bocharov, Kelly, and Eisen.

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.

PETITIONER:

W. Karl Renner
Thomas Rozylowicz
Nicholas Stephens
FISH & RICHARDSON P.C.
axf-ptab@fr.com
tar@fr.com
nstephens@fr.com

PATENT OWNER:

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