

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU, INC.,
Petitioner,

v.

VIDEOLABS, Inc.,
Patent Owner.

IPR2024-01026
Patent 8,667,304 B2

Before KARL D. EASTHOM, STACEY G. WHITE, and BRIAN P.
MURPHY, *Administrative Patent Judges*.

MURPHY, *Administrative Patent Judge*.

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

I. INTRODUCTION

Roku, Inc. (“Petitioner”) filed a Petition pursuant to 35 U.S.C. § 311 requesting institution of *inter partes* review of claims 5–8 and 16–19 (the “challenged claims”) of U.S. Patent No. 8,667,304 B2 (Ex. 1001; “the ’304 patent”). Paper 2 (“Pet.”). VideoLabs, Inc. (“Patent Owner”) timely filed a Patent Owner Preliminary Response. Paper 6 (“Prelim. Resp.”). Pursuant to authorization from the Board, Petitioner filed a Reply to Patent Owner’s Preliminary Response addressing “unforeseeable” claim construction issues, and Patent Owner filed a Sur-Reply. Papers 7, 8.

We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” Under § 314, the Board may not institute review on fewer than all claims challenged in the petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018). If the Board institutes a review, it will institute “on all of the challenged claims and on all grounds of unpatentability asserted for each claim.” 37 C.F.R. § 42.108(a). Upon consideration of the Petition, the Preliminary Response, Reply, Sur-Reply, and the evidence of record, for the reasons set forth below, we conclude Petitioner has demonstrated a reasonable likelihood of prevailing with respect to at least one challenged claim in the ’304 patent. Accordingly, we institute an *inter partes* review of claims 5–8 and 16–19 of the ’304 patent on all grounds set forth in the Petition. *See* 37 C.F.R. § 42.108(a).

A. Real Parties in Interest and Related Matters

Petitioner, Roku, Inc., identifies itself as the real party in interest. Pet. 7. Patent Owner, VideoLabs, Inc., identifies itself as the real party in interest. Paper 5, 2.

The parties identify the following related matters:

VideoLabs, Inc. v. ASUSTeK Computer Inc., No. 6-22-cv-00720 (W.D. Tex.) (pending);

VideoLabs, Inc. v. HP Inc., No. 6-23-cv-00641 (W.D. Tex.) (pending); and

VideoLabs, Inc., et al. v. Roku, Inc., No. 1-23-cv-01136 (D. Del.) (pending).

Pet. 7; Paper 5, 2.

B. The '304 Patent

The '304 patent, titled “Methods and Apparatuses for Secondary Conditional Access Server,” is directed to techniques “for bridging two security systems so that a primary security system can control premium content distribution to external devices secured by a secondary security system.” Ex. 1001, 2:59–62. The '304 patent discloses a plurality of embodiments. In one embodiment:

[T]he primary security system is a broadcast CA [conditional access] system, used to secure the distribution of premium content only to legitimate *subscribers*; and the secondary security system includes a digital rights management system used to secure the distribution of premium content only to the legitimate *devices* of the subscriber.

Id. at 2:64–3:3 (emphasis added). In another embodiment “the secondary security system includes another broadcast CA system, used to secure the re-distribution of premium content only to the legitimate *local subscribers*” of the second broadcast CA system. *Id.* at 3:7–10 (emphasis added). Either way, the secondary security system acts as a bridge because it is both an authorized client of the primary security system, from which it receives protected content, and a server of protected content to secondary clients, such as authorized subscriber devices in a digital rights management (“DRM”) system or authorized local subscribers in a second broadcast CA system.

Figure 2A of the '304 patent depicts an embodiment of the claimed invention. We reproduce below annotated Figure 2A from the Petition:

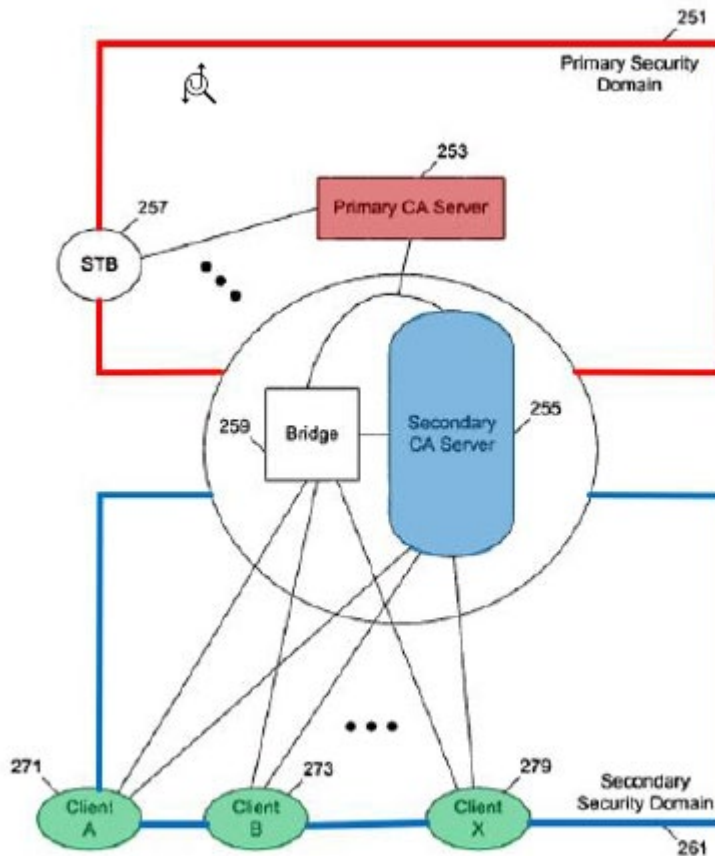


Fig. 2A

Pet. 10. The primary CA server (253, red) controls access to the content in the primary security domain (251), which is “typically a broadcast CA system.” Ex. 1001, 7:8–13. Only an authorized client of the primary security domain, such as set top box (257), can access (decrypt) the primary CA server-protected content. *Id.* at 7:13–17. Secondary CA Server (255, blue) is a bridge that acts as an authorized client of the primary security domain “and as a control information provider of the secondary security domain (261).”¹ *Id.* at 7:37–39. “[T]he secondary CA access clients (e.g., 271, 273, . . . 279, green) in the secondary

¹ Quotations from patent documents may omit or de-emphasize bold numerals.

security domain (261) may access the content secured in the secondary security domain under the control of the secondary CA server (255),” for example by receiving control words from the secondary CA server that permit the secondary clients to decrypt the content. *Id.* at 7:26–31, 44–52.

C. Illustrative Claim

Claims 5 and 8 are the independent claims challenged in this Petition.

Claim 5, reproduced below, illustrates the claimed subject matter:

5[pre.i]² A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server

5[pre.ii] wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and

5[pre.iii] wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:

5[a] receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and

5[b] receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the

² We adopt Petitioner’s claim limitation identifiers for convenience.

second conditional access client being in the second security domain.

Ex. 1001, 25:41–64 (emphasis added).

D. Asserted Grounds of Unpatentability

Petitioner asserts claims 5–8 and 16–19 are unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/ Basis
5-6, 8, 16-17, 19 (Ground 1)	102 ³	Russ ⁴
5-6, 8, 16-17, 19 (Ground 2)	103	Russ
7, 18 (Ground 3)	103	Russ, Robert ⁵

Pet. 9. Petitioner relies on the Declaration testimony of Anthony J. Wasilewski, Ph.D. in support of the asserted unpatentability of the challenged claims. Ex. 1003. Patent Owner relies on the Declaration testimony of Sam Malek, Ph.D. in opposition. Ex. 2001.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner describes a person of ordinary skill in the art (“POSA”) as someone having “a bachelor’s degree in computer science, electrical engineering, or a related field, and approximately two or more years of experience in multi-

³ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), includes revisions to 35 U.S.C. §§ 102, 103 that became effective after the filing of the application that led to the challenged patent. Hence, this *inter partes* review is governed by the pre-AIA provisions of 35 U.S.C. §§ 102, 103.

⁴ US Patent No. 6,748,080 B2 issued June 8, 2004, filed May 24, 2002 (Ex. 1005, “Russ”).

⁵ US Patent No. 7,546,641 issued June 9, 2009, filed Feb. 13, 2004 (Ex. 1006, “Robert”).

media content distribution and management. Additional education could substitute for professional experience, and vice versa.” Pet. 14–15. Patent Owner and its expert, Dr. Sam Malek, apply Petitioner’s proposed definition for purposes of its Preliminary Response. Prelim. Resp. 5 (citing Malek Dec. Ex. 2001 ¶ 38).⁶

In determining the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). “These factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art.” *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). There is uncontested evidence in the record before us that reflects the knowledge and experience of a POSA.

We adopt Petitioner’s proposal for purposes of institution, which the prior art of record supports. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579

⁶ Contrary to Patent Owner’s contention that Petitioner does not show that Dr. Wasilewski “qualifies as a POSITA,” his physics degree, background, and experience in systems involving multi-media content distribution and management and/or related fields, including as an inventor of over 50 patents in fields that include encryption, MPEG systems, and transfer of digital content, including Russ (Ex. 1005), along with extensive engineering experience in related fields, is more than adequate on this preliminary record to qualify Dr. Wasilewski as an artisan of ordinary skill. *Compare* Prelim. Resp. 5, with Ex. 1003 ¶¶ 4–19 and Ex. 1004.

F.2d 86, 91 (CCPA 1978).

B. Claim Construction

We construe claim terms 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). In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a POSA at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). “Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.” *Id.* at 1313. The “specification ‘is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.’” *Id.* at 1315 (citation omitted). Accordingly, when construing a disputed claim limitation, “we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

At Petitioner’s request, we authorized the parties to file a five-page Reply and Sur-Reply “related only to claim construction issues.” Ex. 3002. As stated in our email instructions to counsel, we consider only the parties’ arguments bearing on claim construction and disregard everything else.⁷ The parties direct our attention in particular to the proper construction of an “*independent*” second root of trust in context of the recited claim limitation: “ . . . *receiving, at a second conditional access client of the second conditional access server, an authentication*

⁷ The parties are reminded of the Board’s sanction authority for non-compliance. 35 U.S.C. § 316(a)(6); 37 C.F.R. § 42.12(a)(1).

through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust.” We refer to this disputed claim limitation hereafter as the “*independent authentication*” limitation.

Petitioner proposes the following construction: “authentication processes that are performed by independent roots of trust—*i.e.*, roots of trust with trust determinations that are independent of the outcome of the other.” Reply 3 (citing Ex. 1001, 8:16–38 (“the secondary CA server follows rules (e.g., CA messages) of the primary CA server to manage a secondary subscriber management system”)); *see also id.* at 4 (“‘Independent’ . . . identifies how the first and second roots of trust arrive are used to arrive at their first and second authentication determinations, without relying on the output of the other.”). Petitioner also asserts that Patent Owner’s patentability argument hinges on a construction of “*independent*” such that “‘independent’ as used to modify the first and second roots of trust must be construed as ***independently controlled***,” which Petitioner asserts is inconsistent with the ’304 patent claim language and specification. *Id.* at 1. Patent Owner, for its part, denies that it is advocating for a construction where the two roots of trust are “independently controlled.” Sur-Reply 2–3. Patent Owner does not offer a construction of the “*independent authentication*” limitation, citing an unilluminating description where “the client authentication in the secondary security domain is completely independent from the client authentication in the primary security domain.” *Id.* at 3 (citing Ex. 1001, 8:33–35).

On the present record, we determine that no explicit construction of claim terms is necessary to determine whether to institute an *inter partes* review in this case. *See, e.g., Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed.

Cir. 2011) (“[C]laim terms need only be construed ‘to the extent necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). The parties are ordered to propose and support a specific plain meaning or other construction of the “*independent authentication*” limitation in their briefs, with reference to the following claim language:

5[a] *receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust.*

The parties are ordered to analyze the relevant claim language, and cite to the specification and prosecution history in support of their claim construction where applicable. The parties are further ordered to address the question of whether an “*independent*” “*second authentication process*” and “*second root of trust*” requires a conditional access server that manages a secondary subscriber management system where a “*client*” of the conditional access server does not subscribe to the primary subscriber management system. *See* Ex. 1001, 8:3–38 (e.g., “authentication methods used by the secondary CA server in the secondary subscriber management system are independent from those used by the primary CA server”).

C. Asserted Anticipation of Claims 5–6, 8, 16–17, 19 By Russ (Ground 1)

Petitioner contends that claims 5, 6, 8, 16, 17, and 19 of the ’304 patent are anticipated by Russ. Pet. 17–47. Petitioner provides detailed claim charts mapping the language recited in the challenged claims to the disclosures in Russ with citations to Dr. Wasilewski’s testimony in support. *Id.* at 20–47. Given the similarities in claim language, Petitioner addresses claims 16, 17, and 19 by

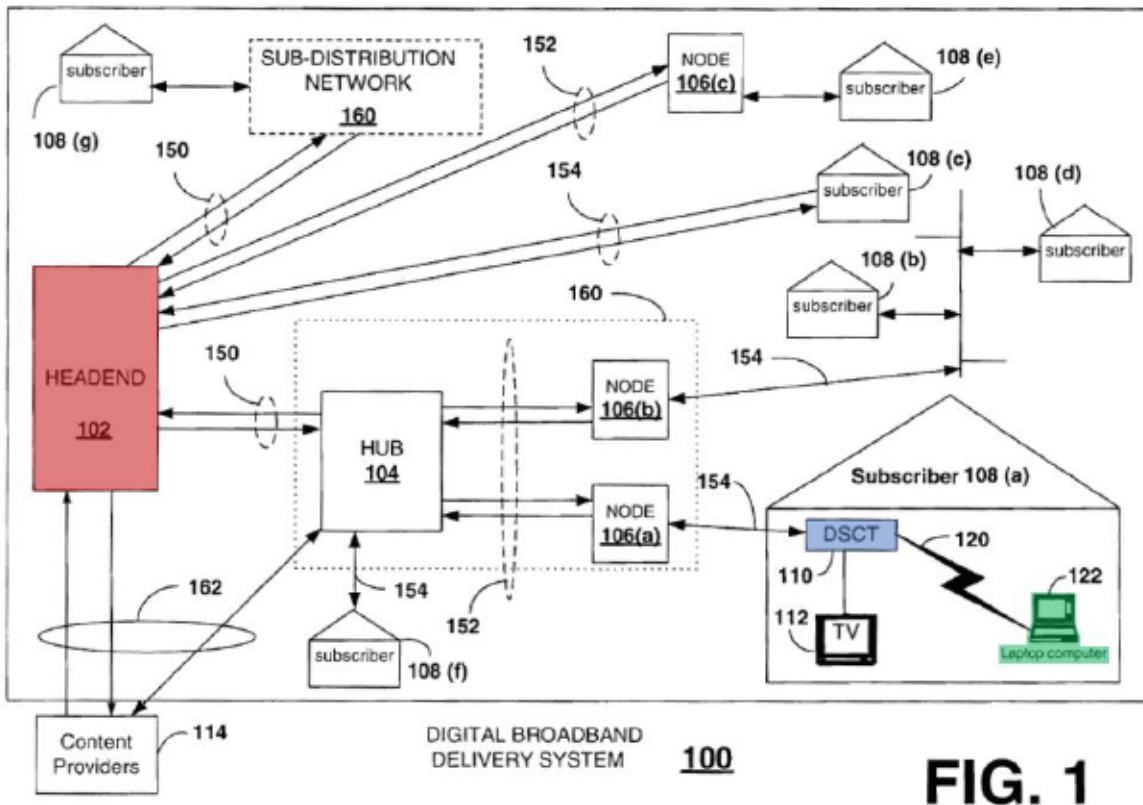
providing cross-citations to its argument and evidence regarding claims 5, 6, and 8. *Id.* at 44–47.

Anticipation under 35 U.S.C. § 102 requires “the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim.” *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010); *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). To anticipate a patent claim under 35 U.S.C. § 102, “a reference must describe, either expressly or inherently, each and every claim limitation and enable one of skill in the art to practice an embodiment of the claimed invention without undue experimentation.” *American Calcar, Inc. v. Am. Honda Motor Co.*, 651 F.3d 1318, 1341 (Fed. Cir. 2011) (citing *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009)). “[E]xtrinsic evidence may be considered when it is used to explain, but not expand, the meaning of a reference.” *In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991) (citing *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576–77 (Fed. Cir. 1991)). We conclude that, at this stage of the proceeding and based on the present record, Petitioner has provided sufficient evidence and argument to establish a reasonable likelihood that Russ anticipates the challenged claims of the ’304 patent.

We begin with a discussion of Russ.

1. The Russ Patent (Ex. 1005)

The Russ patent is titled “Apparatus For Entitling Remote Client Devices,” and it is directed to a “master-receiver in a subscriber television network [that] receives service instances and entitlement information from a headend . . . and re-transmits service instances to a client-receiver after dynamic encryption scheme determination.” Ex. 1005, Abstract (code 57). We reproduce below Petitioner’s annotated version of Russ Figure 1:



Pet. 17 (Ex. 1005, Fig. 1). In digital broadband delivery system 100, headend 102 (red) communicates with content providers 114 to obtain services such as broadcasts or video-on-demand, and to serve them to subscribers. Ex. 1005, 5:35–51. The headend provides services to subscriber 108 (a) by establishing a communication path with digital subscriber communication terminal (“DSCT”) 110 (blue) to provide service instances to client-receiver device 122 (green), for example a laptop computer. *Id.* at 5:52–6:32, 6:51–61, 8:38–9:25.

DSCT 110 manages a local network at the subscriber location and acts as the entitlement authority that grants and deletes entitlements to service instances for client-receiver device 122 based on information provided by the headend. *Id.* at 17:61–18:40, 18:60–65. The encryption scheme by which the DSCT and client-receiver communicate is determined dynamically after the client-receiver joins the

DSCT's local network, or for example "when the user of the client-receiver 122 changes from one user channel to another or requests a different type of content." *Id.* at 3:17-20, 16:64-17:60. Depending on the device classification of the client-receiver, e.g., a laptop, PDA, or set-top box, the DSCT communicates with the client-receiver to negotiate and determine an operative encryption scheme, such as secure socket layer or Digital Transmission Content Protection ("DTCP") encryption protocols that are "known to those skilled in the art." *Id.* at 17:4-14. Alternatively, the headend "can also send an EMM [Entitlement Management Message] to the DSCT instructing the processor to no longer determine the encryption scheme for the client-receiver." *Id.* at 25:17-19. "In that case, the headend determines the encryption scheme used to communicate information between the DSCT and the client-receiver." *Id.* at 25:19-22.

2. *Limitations 5[pre.i-pre.iii]*

Limitation 5[pre.i]: "*A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server*"

Petitioner asserts that Russ discloses a "*non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system,*" in the form of "software stored in memory and executed by a processor, secure element, and cryptographic device to implement logic steps." Pet. 20-21 (citing Ex. 1003 ¶¶ 79-80; Ex. 1005, 3:23-40). Petitioner also asserts that Russ discloses "*a client system in a second security domain to present content provided by a first conditional access server*" because DSCT 110 "provides . . . service instances to client-receiver 122, to which it 'has the authority and capacity to grant and delete entitlements.'" *Id.* (citing Ex. 1003

¶¶ 71–78; Ex. 1005, 5:35–39, 8:49–51, 17:61–18:51); *see also id.* at 26 (citing Ex. 1005, 26:61–67). Petitioner avers that headend 102 is a “*first conditional access server*” providing content. *Id.* at 21 (citing Ex. 1005, 8:8–37, 10:48–65); *see also id.* at 26–28 (citing Ex. 1005, 7:56–8:3, 8:8–37, 10:48–65, 17:61–18:66, Fig. 1). Petitioner further avers that DSCT 110 and client-receiver 122 are in “*a second security domain*,” because “they communicate securely with an encryption scheme that is specifically negotiated and established as between DSCT 110 and client-receiver 122” when it joins the DSCT’s local network at the subscriber location. *Id.* at 20–21 (citing Ex. 1003 ¶¶ 72–77; Ex. 1005, 16:64–17:34, 20:12–24); *see also id.* at 21–25 (further citing Ex. 1005, 7:58–8:3, 8:8–37, 8:49–9:7, 10:48–65, 17:61–18:66, Figs. 1, 5).

Patent Owner does not address limitation 5[pre.i]. Prelim. Resp. 22.

On the present record, we determine Petitioner’s argument and supporting citations to Russ and the Wasilewski Declaration adequately support Petitioner’s assertion that Russ discloses limitation 5[pre.i].

Limitation 5[pre.ii]: “*wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and*”

Petitioner asserts that Russ discloses a headend (“*the first conditional access server*”) that “authenticates a DSCT 110 by verifying that DSCT 1[1]0’s unique serial number is in a database of serial numbers and corresponding keys that have been certified by the manufacturer, and then providing a new trusted DBDS 100 public key to the DSCT 1[1]0; DBDS 100 registers DSCT 1[1]0 as a client to receive service instances” (“*has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust*”).” Pet. 28–29 (citing Ex. 1003 ¶¶ 81–85; Ex. 1005, 7:21–39, 7:56–8:3,

10:39–47). Petitioner argues that a “POSA would have recognized [a “*root of trust*”] as at least including hardware, software, and/or firmware-based systems for establishing trustworthy identities of components or entities, as in Russ.” *Id.* at 29 (citing Ex. 1003 ¶ 83); *see also id.* at 30–32 (mapping a “*first root of trust*” to Russ (citing Ex. 1005, 7:21–8:3, 10:39–47)). Petitioner further contends that the headend in Russ “implements conditional access authority (CAA) logic to control access to service instances for a plurality of DSCTs 110” through an exchange of public keys (“*a first security domain*”). *Id.* at 28–29 (citing Ex. 1003 ¶¶ 81–85); *see also id.* at 29–30 (mapping “*a first security domain*” to Russ (citing Ex. 1005, 6:62–7:6, 8:8–22)).

Patent Owner does not address limitation 5[pre.ii]. Prelim. Resp. 22.

On the present record, we determine Petitioner’s argument and supporting citations to Russ and the Wasilewski Declaration adequately support Petitioner’s assertion that Russ discloses limitation 5[pre.ii].

Limitation 5[pre.iii]: “*wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:*”

Petitioner asserts Russ discloses that when the DSCT (“*a second conditional access server*”) receives a service instance from the headend, the DSCT “decrypts the service instance, then encrypts the service instance with an encryption scheme specifically negotiated between DSCT 110 and client-receiver 122 (“*is configured to substitute the first security domain with the second security domain for client devices*”). Pet. 32 (citing Ex. 1003 ¶¶ 86–90; Ex. 1005, 8:49–9:7, 15:46–54, 19:50–20:19); *see also id.* at 33 (mapping “*the first security domain*” to Russ (citing Ex. 1005, 11:37–46, 13:12–34)), 34–36 (mapping “*configured to substitute the first security domain with the second security domain for client devices*” to

Russ (further citing Ex. 1005, 15:46–54, 19:50–20:19, Fig. 6)). Petitioner argues that the client-receiver is “under a second root of trust established with DSCT 110 via DTCP authentication and based on an Authentication and Key Exchange (AKE) using DTLA licensed certificates” (“*under a second root of trust*”). *Id.* at 32 (citing Ex. 1003 ¶¶ 91–94). Petitioner further argues that a “POSA would have recognized that DTCP protocols include authentication and key and certificate exchange procedures that ensure communications are protected.” *Id.* at 32–33 (citing Ex. 1003 ¶¶ 91–93; Ex. 1010 ¶ 9, Ex. 1011 ¶¶ 53, 107, 139–143, Fig. 17); *see also id.* at 34 (mapping “*the second security domain*” to Russ (citing Ex. 1005, 16:64–17:34)).

Patent Owner does not address limitation 5[pre.iii]. Prelim. Resp. 22.

On the present record, we determine Petitioner’s argument and supporting citations to Russ and the Wasilewski Declaration adequately support Petitioner’s assertion that Russ discloses limitation 5[pre.iii].

3. The “*independent authentication*” limitation 5[a]

Petitioner maps the “*independent authentication*” limitation 5[a] to Russ’s disclosure of an embodiment where the DSCT dynamically determines a DTCP encryption protocol for communicating protected content to the client-receiver. Pet. 36–37 (citing Ex. 1005, 16:64–17:14). Petitioner also cites extrinsic evidence to support its assertion that the disclosed DTCP encryption protocol requires an authentication and key exchange between the DSCT and client-receiver, “thereby explaining what the phrase [DTCP encryption protocol] would have meant to one skilled in the art.” *In re Baxter*, 952 F.2d at 390; *see also* Ex. 1003 ¶¶ 91–92 (“DTCP protocols require that devices undergo a handshaking process, known as an Authentication and Key Exchange (AKE), before protected communications are to take place. A [POSA] would have been familiar with such processes”)

(citing Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107; Ex. 1012 ¶ 41), 93–97. Petitioner asserts the extrinsic evidence demonstrates a “POSA would have recognized that DTCP protocols include authentication and key and certificate exchange procedures that ensure communications are protected.” Pet. 37 (citing Ex. 1003 ¶ 96; Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107, 139–143, Fig. 17).

Patent Owner argues that Petitioner has not provided sufficient evidence to establish that Russ discloses or teaches at least the “*independent authentication*” limitation. Prelim. Resp. 13–22. Patent Owner argues in particular that Russ does not disclose or teach a “*second root of trust*” because “Russ does not mention an ‘Authentication and Key Exchange (AKE)’ or ‘DTLA [Digital Transmission Licensing Authority] licensed certificates’ at all.” *Id.* at 14 (citing Malek Dec. Ex. 2001 ¶ 50). Patent Owner urges that, although Russ discloses a DTCP encryption scheme, Russ “never discloses using it for any *authentication*” because the headend authenticates the client-receiver when it joins the DSCT-managed local network at the subscriber location by “exchanging trusted keys without the need for DTLA certificates.” *Id.* at 15 (citing Ex. 2001 ¶ 54).

a. “second root of trust”

Russ expressly discloses and teaches a DTCP encryption scheme to protect content transmitted from the DSCT to a client-receiver, and Russ does not expressly disclose the use of AKE key exchange and a DTLA license certificate as a “*second root of trust*” for authenticating the client-receiver. Ex. 1005, 16:64–17:14. Nevertheless, Petitioner provides extrinsic evidence to explain the meaning of Russ’s disclosure to a POSA, who Petitioner asserts “would have recognized that DTCP protocols include authentication and key and certificate exchange procedures.” Pet. 37 (citing Ex. 1003 ¶ 96); *see also In re Baxter*, 952 F.2d at 390 (extrinsic evidence may “explain, but not expand, the meaning of a reference”).

Dr. Wasilewski, moreover, cites corroborating documentary evidence to support his opinion that “DTCP protocols require that devices undergo a handshaking process, known as an Authentication and Key Exchange (AKE),” including authentication of the client-receiver by the DSCT (via DTLA license certificate), and that a POSA “would have been familiar with such processes.” Ex. 1003 ¶¶ 91–92 (citing Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107; Ex. 1012 ¶ 41). Dr. Wasilewski further opines that the DTCP/DTLA protocol and license certificate serves as a “*second root of trust*” that is “*independent of and different than*” the first root of trust in Russ “because headend 102 is not disclosed as using any DTCP-related protocols with respect to DSCT 110.” *Id.* ¶¶ 92–93.

At this stage, Patent Owner disputes Petitioner’s evidence that a POSA would have recognized Russ’s disclosure of DTCP encryption as requiring AKE key exchange via DTLA license certificate as a “*second root of trust*” for authenticating the client-receiver. For example, Patent Owner relies on Dr. Malek’s opinion that “Russ discloses exchanging trusted keys without the need for DTLA certificates” to rebut Dr. Wasilewski’s sworn testimony. Prelim. Resp. 15 (citing Ex. 2001 ¶ 54). Patent Owner and Dr. Malek, however, do not specifically address Petitioner’s extrinsic evidence that DTCP encryption requires an AKE key exchange and a DTLA license certificate. *See* Prelim. Resp. 15 (citing Ex. 2001 ¶ 54) & n.1 (acknowledging that Petitioner cites two patent publications without addressing their teachings as relied upon by Petitioner, or Dr. Wasilewski’s testimony about them). Patent Owner also relies on Russ’s description of the headend authenticating the client-receiver with an exchange of trusted public keys when the receiver “device comes online,” but without explaining what impact, if any, the initial registration of the client-receiver would have on the use of AKE key exchange and DTLA license certificate authentication

in a DTCP encryption scheme. *Id.* at 15–16 (citing Ex. 1005, 26:29–48; Ex. 2001 ¶ 54).

Accordingly, at this stage of the proceeding, Dr. Wasilewski’s testimony and corroborating evidence sufficiently establish that: i) Russ’s disclosed DTCP encryption scheme requires AKE key exchange and a DTLA license certificate as a “*second root of trust*” in a “*second authentication process*” for authenticating the client-receiver, and ii) a POSA would have recognized that fact. *See In re Baxter*, 952 F.2d at 390 (“the dispositive question regarding anticipation [is] whether one skilled in the art would reasonably understand or infer [the asserted disclosure] from the [prior art’s] teaching”).

b. “independent” “second root of trust” and “authentication”

Petitioner argues that DTCP authentication based on AKE key exchange using DTLA license certificates is “independent and different than the first authentication process’s and the first root of trust’s use of serial numbers and keys between the headend 102 and DSCT 110 discussed in claim 5[pre.iii].” Pet. 36–37 (citing Ex. 1003 ¶¶ 95–97; Ex. 1005, 16:64–17:14; Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107, 139–143, Fig. 17). Dr. Wasilewski explains that “because headend 102 is not disclosed as using any DTCP-related protocols with respect to DSCT 110, the authentication between DSCT 110 and client-receiver 122 is independent and different from that between headend 102 and DSCT 110.” Ex. 1003 ¶ 96. Dr. Wasilewski opines, therefore, that “the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust, as claimed.” *Id.* ¶ 97. Petitioner also maintains “all that is required is” the two roots of trust “are independent of the outcome of the other.” Reply 3.

Patent Owner contends the alleged “*second root of trust*” identified by Petitioner is not “*independent*” of the first root of trust used by the headend to authenticate the DSCT. Prelim. Resp. 16–22. Patent Owner cites the distinction made during prosecution that “a ‘child client public key’ may have been different, but was not independent,” in support of the argument. *Id.* at 17 (citing Ex. 1015, 477–488). Patent Owner appears to be equating Russ with the Simelius parent-client/child-client voucher verification system where “the child client public key is chaining to the root of trust of the content server,” as argued by the applicant during prosecution. Ex. 1015, 477; Prelim. Resp. 20. Patent Owner reasons that in Russ, according to Petitioner’s theory, “the roots of trust are not independent, they are ‘chained,’ much like the art distinguished in prosecution.” Prelim. Resp. 20.

Patent Owner further contends the headend “controls any authentication of a client-receiver [and] what content it can receive,” and “even the dynamic encryption is controlled by the headend.” *Id.* at 18–19 (citing Pet. 40, Ex. 1005, 7:56–8:3, 14:50–55; 25:17–22). Patent Owner reasons that because “Russ’s headend 102 controls the entire DBDS network, any second root of trust between the DSCT 110 and client-receiver 122 . . . cannot be *independent* of the alleged first root of trust.” *Id.* at 20–21. Patent Owner also argues Russ does not disclose two “*independent*” roots of trust because “Russ teaches a single ‘subscriber network’ that is under the control of a single system operator” where “all client-receivers are devices of a subscriber to the DBDS system.” *Id.* at 21 (citing Ex. 2001 ¶ 44).

At this stage of the proceeding, Patent Owner disputes Petitioner’s contention in part based on the meaning of “*independent*” in the “*independent authentication*” limitation, but without offering a plain meaning or proposed construction. For example, it is unclear if Patent Owner is arguing that the

“*independent authentication*” limitation should be construed as limited to a bridge between a primary subscriber management system and a secondary subscriber management system for users who are not subscribers to the primary system. We understand Patent Owner’s argument to exclude a single subscriber management system, such as Russ discloses, from anticipating the challenged claims, articulated as follows:

The ’304 patent . . . teaches how to bridge together different networks under different control. . . . In Russ, all client-receivers are devices of a subscriber to the DBDS system. However, “[a]n advantage to the present bridging service [of the ’304 patent] allows a user to receive secured content from a primary system without directly subscribing to the primary system services.” EX1015, 479. This is made possible by having “two independent authentication processes that use two different and independent roots of trust.” *Id.* This purpose of the ’304 patent is the antithesis of Russ, which discloses only one system operator verifying subscribers and controlling all functionality and content within a single Digital Broadband Delivery System subscriber network. *See, e.g.*, EX1005, 10:25-29.

Prelim. Resp. 21; *see also* Sur-Reply, 3 (citing Ex. 1001, 8:33–35 (“[T]he client authentication in the secondary security domain is completely independent from the client authentication in the primary security domain.”)).

Patent Owner does not analyze in detail the recited claim language or the corresponding written description, e.g., in column 8 of the ’304 patent specification, regarding the use of a conditional access server to bridge two different networks under different control using two “*independent*” authentication processes. Patent Owner does rely on the prosecution history (Ex. 1015) in an attempt to distinguish Russ from the ’304 patent claims, in what reads as an argument for prosecution history estoppel or disclaimer. *See Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 722, 733 (2002) (“Prosecution history estoppel requires that the claims of a patent be interpreted in light of the

proceedings in the PTO during the application process.”); *Uship Intellectual Props., LLC v. United States*, 714 F.3d 1311, 1313 (Fed. Cir. 2013) (exception to general rule of ordinary and customary meaning “when the patentee disavows the full scope of a claim term either in the specification or during prosecution”). The parties should address the ’304 patent claim language, specification, and prosecution history in detail, including whether, and to what extent, any relevant subject matter was disavowed, disclaimed, or otherwise excluded during prosecution.

Patent Owner also argues that Russ’s headend “determines the encryption scheme used to communicate information between DSCT 110 and the client-receiver 122,” and that Russ’s “headend controls encryption.” Prelim. Resp. 10–11 (citing Ex. 1005, 25:17–22). Patent Owner’s argument, however, is not consistent with Russ, which states:

The system controller [in the headend] “*can also send* an EMM to the DSCT instructing the processor to *no longer determine* the encryption scheme for the client-receiver. *In that case*, the headend determines the encryption scheme used to communicate information between the DSCT and the client-receiver.

Ex. 1005, 25:17–22 (emphasis added). Russ makes clear that headend determination of the encryption scheme for communicating with the client-receiver is an alternative to DSCT control via dynamic encryption determination in communication with the client-receiver.⁸

⁸ In addition to dynamic encryption control using DTCP protocols and known schemes that include authentication and encryption, Russ generally discloses the use of different EMMs for communicating between headend 102 and DSCT 110, between headend 102 and client receiver 122, and between DSCT 110 and client-receiver. See Ex. 1005, 20:11–47.

Patent Owner then argues that because Russ's headend controls the encryption scheme, initial connection, and conditional access authority, the "DSCT simply 'acts as a proxy' at the behest of the headend," a prior art feature that Patent Owner alleges was distinguished during prosecution of the '304 patent. Prelim. Resp. 13 (citing Ex. 1015, 478; Ex. 1005, 2:55–3:10, 19:24–26). Russ is not consistent with Patent Owner's argument because Russ discloses that the DSCT acts as a proxy only *when* the headend, rather than the DSCT, determines the encryption scheme for the client-receiver. Ex. 1005, 19:16–27 ("In one preferred embodiment, . . . *when* the headend decides to entitle the client receiver for the requested service, the headend *can also* determine the encryption scheme for the selected service. *In this case*, the DSCT acts as a proxy for the client-receiver" (emphasis added)). When the DSCT dynamically determines the DTCP encryption scheme for communicating with the client-receiver, as asserted by Petitioner, the DSCT does not act as a proxy for the headend.

At this stage of the proceeding, the evidence of record supports Petitioner's contention that Russ discloses the "*independent authentication*" limitation challenged by Patent Owner. The "*first root of trust*" derives from "DSCT 110's unique serial number [] in a database of serial numbers and corresponding keys that have been certified by the manufacturer, and then providing a new trusted DBDS 100 public key to the DSCT 110." Pet. 28–29 (citing Ex. 1003 ¶¶ 81–85; Ex. 1005, 7:21–39, 7:56–8:3, 10:39–47). "[T]he manufacturer is a key certification authority that certifies to the operator of the DBDS 100 that a given public key belongs to a specific DSCT 110." Ex. 1005, 7:35–37. The "*second root of trust*" is "*independent of and different than the first root of trust*" because the second root of trust derives from client-receiver "device identification numbers embedded in a device certificate issued by a licensing institution such as the

DTLA” using the DTCP communication sequence. Pet. 32–33 (citing Ex. 1003 ¶¶ 86–94; Ex. 1005, 16:64–17:34; Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107, 139–143, Fig. 17). “DSCT 110 and client-receiver [122] utilize DTCP authentication based on a root of trust established by DTCP/DTLA protocols and certificates, . . . [which] is independent and different from that between headend 102 and DSCT 110” Ex. 1003 ¶ 96; *see also* Pet. 36 (“DTCP authentication is based on an Authentication and Key Exchange (AKE) using DTLA licensed certificates, which is independent and different than the first authentication process’s and the first root of trust’s use of serial numbers and keys between the headend 102 and DSCT 110”). In addition, Dr. Malek does not dispute that the two roots of trust identified by Petitioner are “*different*,” and he does not testify that Russ’s system derives one root of trust from the other when the DSCT adopts the DTCP communication sequence to communicate protected content to the client-receiver. *See* Ex. 2001 ¶¶ 53–62.

4. Limitation 5[b]

Limitation 5[b]: “*receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.*”

Petitioner asserts that Russ discloses the client-receiver (“*the second conditional access client*”) “receives a service instance from DSCT 110” (“*receiving . . . content*”) “using, *e.g.*, a DTCP access controlled format” (“*that is in an access controlled format*”). Pet. 37 (citing Ex. 1003 ¶¶ 98–103). Petitioner further asserts that Russ discloses the “DSCT 110 formats the service instance for transmission using the determined encryption scheme” (“*specified by the second conditional access server*”) such that “DSCT 110 and client-receiver 122 are in the

second security domain” (“*in the second security domain, the second conditional access client being in the second security domain*”). *Id.* Petitioner further emphasizes Russ’s disclosure that “DSCT 110 may thus determine to use an encryption scheme based on DTCP protocols.” *Id.* (citing Ex. 1003 ¶ 99; Ex. 1005, 16:64–17:47); *see also id.* at 38–40 (citing Ex. 1003 ¶¶ 100–101; Ex. 1005, 16:64–17:47, 20:12–24, Fig. 6).

Patent Owner does not directly address limitation 5[b]. Prelim. Resp. 13–22.

On the present record, we determine Petitioner’s argument and supporting citations to Russ and the Wasilewski Declaration adequately support Petitioner’s assertion that Russ discloses limitation 5[b].

5. Claims 6 and 8

Petitioner contends claims 6 and 8, both of which depend from claim 5, are anticipated by Russ. Pet. 40–44 (citing Ex. 1003 ¶¶ 104–11). Claim 6 recites “*wherein the second conditional access client does not have a user key representing a subscriber of the first security system,*” and claim 8 recites “*wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.*” In addition to Dr. Wasilewski’s declaration testimony, Petitioner supports its contentions with citations to specific disclosures in Russ. *Id.* (citing Ex. 1005, 7:56–58, 8:49–9:7, 12:47–13:19, 15:46–54, 16:64–17:14, 19:50–20:19, 20:47–53, 26:16–28, Fig. 6). Petitioner further provides claim chart cross-reference citations to the arguments and evidence for anticipation of claims 5, 6, and 8, in support of its contention that Russ discloses

the limitations recited in challenged claims 16, 17, and 19. *Id.* at 44–47 (citing Ex. 1003 ¶¶ 112–119).

Patent Owner does not directly address claims 6, 8, 16, 17, or 19. Prelim. Resp. 13–22.

On the present record, we determine Petitioner’s argument and supporting citations to Russ and the Wasilewski Declaration adequately support Petitioner’s assertion that Russ discloses the limitations recited in claims 6, 8, 16, 17, and 19.

6. Conclusion

In conclusion, Petitioner provides detailed argument and evidence, including expert testimony from Dr. Wasilewski with corroborating documentary evidence, in support of its assertion that Russ anticipates the challenged claims. Pet. 17–47 (citing Ex. 1003 ¶¶ 59–119). As addressed above, Patent Owner challenges Petitioner’s mapping of the “*independent authentication*” limitation 5[a], particularly the “*independent*” “*second root of trust*,” to the cited disclosure in Russ. On the present record, we find Petitioner’s argument and evidence adequately support Petitioner’s assertion that Russ discloses all limitations recited in the challenged claims. Therefore, on the present record, we determine Petitioner’s argument and evidence demonstrate a reasonable likelihood it would prevail in showing the unpatentability of claims 5, 6, 8, 16, 17, and 19 of the ’304 patent as anticipated by Russ.

D. Asserted Obviousness of Claims 5–6, 8, 16–17, 19 of the ’304 patent Over Russ (Ground 2)

A petition for *inter partes* review must identify “with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim.” 35 U.S.C. § 312(a)(3); *see also* 37 C.F.R. § 42.104(b) (specifying necessary elements of a

petition); *Adaptics Ltd. v. Perfect Co.*, IPR2018-01596, Paper 20, 15 (PTAB Mar. 6, 2019) (informative) (quoting 35 U.S.C. § 312(a)(3)). 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). “It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016). “[T]he expedited nature of IPRs bring with it an obligation for petitioners to make their case in their petition to institute. While the Board’s requirements are strict ones, they are requirements of which petitioners are aware when they seek to institute an IPR.” *Id.*

Petitioner presents a vague “catch-all” obviousness argument based on Russ, arguing that “Russ further teaches that its disclosed features are combinable, and a POSA would have thus found the claims obvious as well.” Pet. 48. Rather than provide a particularized argument setting out the evidence demonstrating how specific features and embodiments disclosed in Russ might be combinable, Petitioner relies instead on generic statements that “various examples and embodiments disclosed in Russ are directly related to each other,” contending that a POSA would have “exercised routine experimentation in implementing a system based on Russ’s disclosure and combined features from related ‘examples’ or ‘embodiments’ to result in a desired system or functionality.” *Id.*

We agree with Patent Owner that Petitioner’s Ground 2 “vaguely argues that it would have been obvious to combine” the different embodiments disclosed in Russ. Prelim. Resp. 22; see *Google LLC v. MindbaseHQ, LLC*, IPR2021-01251 Paper 40, 56 (PTAB Jan. 6, 2023) (asserted inherency ground in petition was

“confusing and vague”). The record supports Patent Owner’s argument. Petitioner also fails to identify any differences between the prior art Russ patent and the challenged claims. Therefore, we determine Petitioner’s argument and evidence do not demonstrate a reasonable likelihood it would prevail in showing the unpatentability of claims 5–6, 8, 16–17, 19 of the ’304 patent as obvious over Russ.

E. Asserted Obviousness of Claims 7 and 18 of the ’304 patent Over Russ in view of Robert (Ground 3)

Petitioner contends that claims 7 and 18 of the ’304 patent would have been obvious over Russ in view of Robert. Pet. 49–56. Claim 7 depends from claim 5, and claim 18 depends from claim 16. Claims 7 and 18 both recite: “*wherein the content comprises a decrypted version of an entitlement control message.*” Petitioner provides detailed claim charts for both claims. *Id.* at 54–56.

We begin with a discussion of Robert.

1. Robert (Ex. 1006)

Robert, titled “Conditional Access to Digital Rights Management Conversion,” is directed to providing security of digital content by unifying aspects of a conditional access (CA) protection scheme and a digital rights management (DRM) scheme. Ex. 1006, 1:60–2:19. CA systems are “used in broadcast platforms to securely deliver content from a service operator, such as a satellite or cable provider, to individual receivers.” *Id.* at 1:30–34. “DRM systems have been developed to securely allow consumption of other types of content (e.g., CDs, MPEG files, DVDs, audio/video streams, etc.) on devices such as personal computers and other electronic items.” *Id.* at 1:48–52. Unifying the two systems includes translating aspects of CA schemes into a DRM-type content license. *See id.* at Fig. 5.

Robert states that “CA and DRM technologies were developed for protecting different types of content with different delivery mechanisms, and thus with different security risks in mind.” *Id.* at 1:60–62. The CA technologies relate to protection systems for broadcast and streamed pay-TV media so that “the various levels of protection (such as the intermittent updated keys and encryption thereof at different times and concealed in different messages) were considered important, possible, and practical.” *Id.* at 1:65–2:2. The DRM technologies relate to “a single piece of content” such that “the binding of the content to a single license and binding the license to a particular device (or group of devices) provides an appropriate level of protection.” *Id.* at 2:7–11. Robert attempts to unify or bridge the two types of protection so that multiple devices in a home may communicate with one another and share content. *See* Ex. 1006, 2:12–19.

Figure 5, showing steps for producing a DRM license according to Robert’s CA protection scheme, follows:

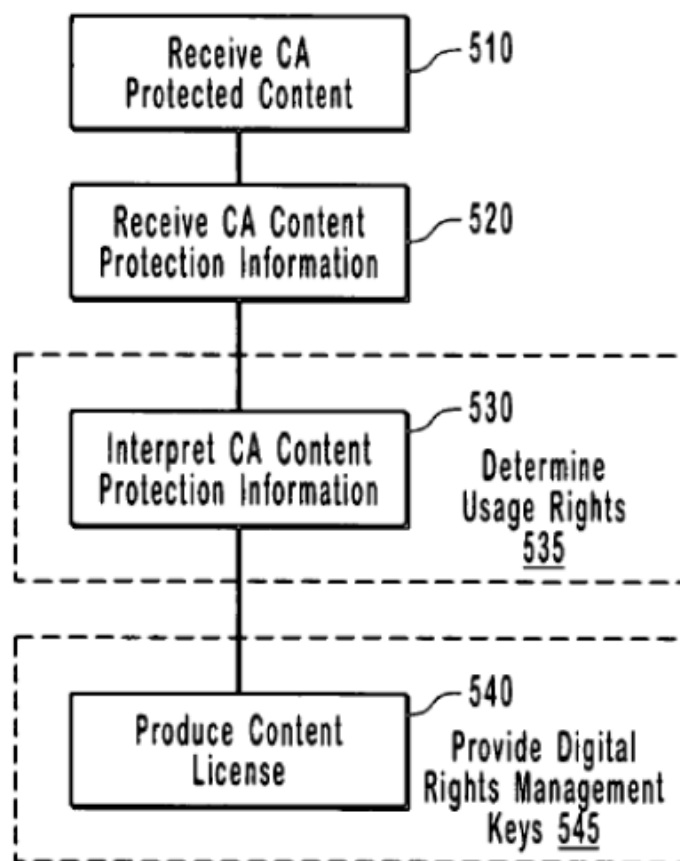


Fig. 5

Figure 5 above shows steps for interpreting CA content protection information—which may define how and under what conditions content may be consumed at a destination device—and producing a content license for enforcing the interpreted rights at a destination device. *See* Ex. 1006, 12:16–26. The method includes “transcribing content protection information from the CA syntax to the DRM syntax,” including control words (CWs) and keys in the DRM license, and decrypting and re-encrypting the CA content with DRM methods. *Id.* at 6:26–59. The embodiment in Figure 5 provides that “the aforementioned steps and acts may also include an act of authenticating that the destination device is a trusted device

for establishing a secure communication channel between a receiver of the conditional access protected content and the destination device.” *Id.* at 12:30–34.

2. *Obviousness analysis*

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time the invention was made. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a)). Obviousness is resolved based on 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) objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). A party who petitions the Board for a determination of obviousness must show 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.” *Procter & Gamble Co. v. Teva Pharms. USA, Inc.*, 566 F.3d 989, 994 (Fed. Cir. 2009) (quoting *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1361 (Fed. Cir. 2007)). We assess Petitioner’s evidence and argument according to the above-referenced standard.

Petitioner demonstrates sufficiently, as discussed in section C above, that Russ anticipates claims 5 and 16 from which claims 7 and 18, respectively, depend. Russ discloses a system where the headend provides service instances (content) and service instance entitlements to the DSCT, which communicates the content and entitlements to the client-receiver under the protection of a dynamically determined encryption scheme. Ex. 1005, 16:64–17:60, 20:12–17,

26:54–64, 26:54–64. With regard to claims 7 and 18—“*wherein the content comprises a decrypted version of an entitlement control message*”—Russ discloses only that the client-receiver decrypts service instances by generating control words. *Id.* at 26:16–28, 26:54–67. Petitioner acknowledges that Russ does not disclose or teach details such as “what specific information or control words client-receiver 122 uses to decrypt service instances.” Pet. 51. Petitioner, however, relies on Robert to fill the disclosure gap in Russ.

Petitioner emphasizes that Robert teaches transmission of CA content to a destination device, including “control words for decrypting content protected by DRM.” Pet. 52 (citing Ex. 1006, 9:53–10:4). Robert teaches a POSA that a destination device obtains a control word by decrypting an Entitlement Control Message (“ECM”) received from the head end such that “the destination device can use a DRM license to decrypt CA-protected content.” *Id.* (citing Ex. 1006, 4:27–33, 6:31–59, 9:66–10:4). For example, as Petitioner argues, the client-receiver in Russ (a destination device in Robert) would receive a control word in an ECM as taught by Robert, decrypt and analyze the ECM, and transmit the “ECM contents including the control word to the destination device, now protected via DRM.” *Id.* at 54 (citing Ex. 1003 ¶¶ 128–133). The client-receiver would “transcribe[] the control word[] into a DRM license such that the destination device [] can decrypt the CA-protected content with the control word[.]” *Id.* (citing Ex. 1006, 6:31–69, 9:53–10:4); Ex. 1003 ¶¶ 129–132.

Petitioner argues that a POSA would have been “motivated to implement Russ with details taught by Robert and transmit control words as access controlled data to client-receiver 122 to facilitate client-receiver 122’s access to encrypted service instances while being protected by the protocols negotiated between DSCT 110 and client-receiver 122.” *Id.* at 52. In addition, Petitioner asserts that a

“DSCT 110 configured to operate . . . in view of Robert’s teachings would not be required to decrypt or descramble a service instance before transmitting it to client-receiver 122, thereby saving system time and resources.” *Id.* at 52–53 (citing Ex. 1005, 19:50–59; Ex. 1003 ¶ 126). Petitioner further argues that a “POSA would have had a reasonable expectation of success implementing Russ’s system by including decrypted ECM information, including control words, as access controlled data,” given that “both Russ and Robert explain that content protection protocols and encryption schemes are well-known processes.” *Id.* at 53 (citing Ex. 1005, 17:7–14; Ex. 1006, 5:10–11).⁹

Patent Owner relies on its arguments and evidence addressed above with respect to anticipation in Ground 1, and, at this stage, does not address the merits of Petitioner’s argument and evidence in support of the asserted obviousness of claims 7 and 18. Prelim. Resp. 22.

For purposes of institution, we determine the preliminary record supports Petitioner’s showing that claims 7 and 18 would have been obvious over Russ and Robert. *See* Pet. 49–56. Based on our review of the present record, we determine Petitioner’s argument and evidence demonstrate a reasonable likelihood it would prevail in showing that claims 7 and 18 would have been obvious over Russ in view of Robert.

⁹ “Typically, ECMs are transmitted without being encrypted so that the DSCTs do not have to spend time decrypting the content of the ECM before generating the control word.” Ex. 1005, 13:23–26; *see also id.* at 13:26–28 (“However, the ECMs include an authentication token that is used for authenticating the message content and limiting access thereto . . .”).

III. CONCLUSION

For the foregoing reasons, we determine Petitioner has established a reasonable likelihood of prevailing in its challenge to the patentability of claims 5–8 and 16–19 of the '304 patent. Therefore, we institute *inter partes* review of the challenged claims.

At this stage of the proceeding, the Board has not made a final determination as to the patentability of any challenged claims or any underlying factual or legal issues. A final determination will be made based on the record as developed during the *inter partes* review. Any final determination will be based on the record developed during trial. Any argument not asserted in a timely-filed brief, such as a response to the Petition, may be deemed forfeited or waived, even if that argument appears in the Preliminary Response.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 5–8 and 16–19 of the '304 patent is instituted with respect to all grounds set forth in the Petition;

FURTHER ORDERED that the parties shall propose and support a specific plain meaning or other construction of the “*independent authentication*” limitation in their briefs; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '304 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

Case IPR2024-01026
Patent 8,667,304 B2

For PETITIONER:

Scott McKeown

Victor Cheung

WOLF, GREENFIELD & SACKS P.C.

Smckeown-ptab@wolfgreenfield.com

Vcheung-ptab@wolfgreenfield.com

For PATENT OWNER:

Jerry Tice

Aaron Hand

BUNSOW DE MORY LLP

jtice@bdiplaw.com

ahand@bdiplaw.com