

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU, INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner.

IPR2024-01024
Patent 8,291,236 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 48–50, 57, 82–84, 91, 116–118, 125, and 140–142 (the “challenged claims”) of U.S. Patent No. 8,291,236 B2 (Ex. 1001; “the ’236 patent”). Paper 2 (“Pet.”). VideoLabs, Inc. (“Patent Owner”) timely filed a Patent Owner Preliminary Response. Paper 7 (“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 8, 10.

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 ’236 patent. Accordingly, we institute an *inter partes* review of claims 48–50, 57, 82–84, 91, 116–118, 125, and 140–142 of the ’236 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. 6.
Patent Owner, VideoLabs, Inc., identifies itself as the real party in interest.
Paper 6, 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. ASUSTeK Computer Inc., No. 6-23-cv00640 (W.D. Tex.)
(voluntarily dismissed);

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 6, 2.

B. The '236 Patent

The '236 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, 2:56–59. The '236 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 2:61–67 (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 3:1–7 (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 '236 patent depicts an embodiment of the claimed invention. We reproduce below annotated Figure 2A from the Petition:

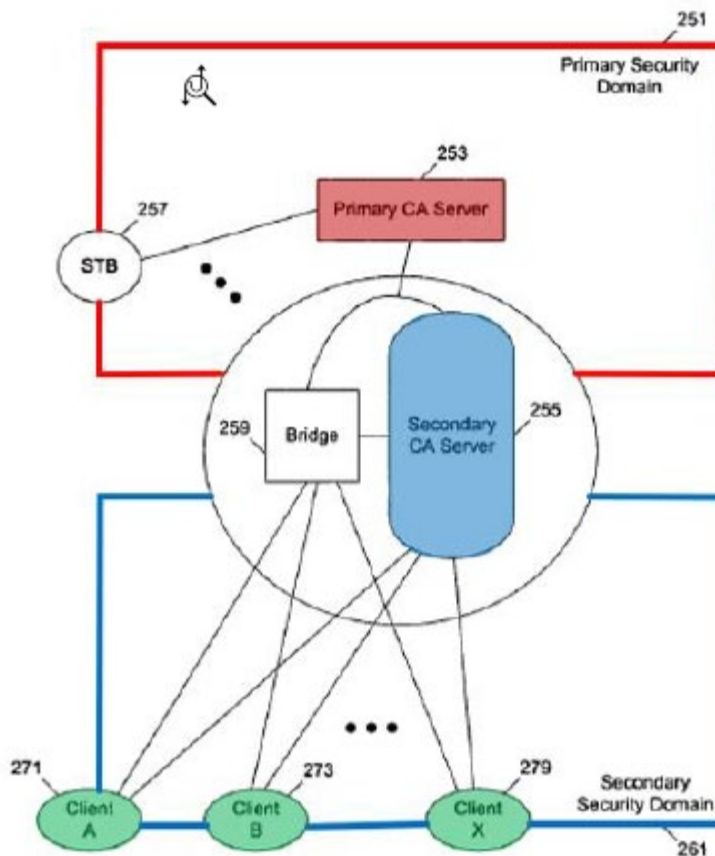


Fig. 2A

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 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 7:23–29, 44–52.

C. Illustrative Claim

Claims 48, 82, 116, and 140 are the independent claims challenged in this Petition. The Petition focuses primarily on claims 140–142 for purposes of argument because the limitations in the other challenged claims “are substantially similar to the functions, steps, and related structures in independent client claim 140 and its dependent claims.” Pet. 51. For its part, Patent Owner focuses on the recited “*second root of trust*” “as required by all challenged claims.” Prelim. Resp. 13, 16. Claim 140, reproduced below, illustrates the claimed subject matter:

140[pre]² A secondary conditional access client, comprising:

140[a.i] a communication interface to receive, from a conditional access server through a network connection, **[a.ii]** access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain; and

140[b] a processor coupled to the communication interface, the processor to process the access controlled data,

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

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

140[c.i] wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and **[c.ii]** the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and *wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust*, and **[c.iii]** wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

Ex. 1001, 41:39–42:10 (emphasis added).

D. Asserted Grounds of Unpatentability

Petitioner asserts claims 48–50, 57, 82–84, 91, 116–118, 125, and 140–142 are unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/ Basis
48–50, 57, 82–84, 91, 116–118, 125, and 140–142 (Ground 1)	102 ³	Russ ⁴
48–50, 57, 82–84, 91, 116–118, 125, and 140–142 (Ground 2)	103	Russ

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.

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”).

1003.⁵ 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-media content distribution and management. Additional education could substitute for professional experience, and vice versa.” Pet. 13–14. 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

⁵ Petitioner filed a Notice Ranking Petitions and Explaining Material Differences. Paper 3. Petitioner states that it filed three parallel IPR petitions challenging three different claim sets of the ’236 patent “solely for word count purposes that preclude all claims from being challenged in [a] single petition,” “there is no duplicative overlap of the same claims across petitions,” and there is a “need to set forth constructions for claim language invoking § 112 ¶ 6.” *Id.* at 1–2 (citing Consol. Tr. Pr. Guide, 59–61). Patent Owner does not address Petitioner’s Notice. We agree with Petitioner’s reasoning and decline to exercise our discretionary denial authority under 35 U.S.C. § 314(c).

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.

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 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: “. . . *a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust 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 5 (“‘Independent’ . . . identifies how the first and second roots of trust 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

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).

with the '236 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 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 4 (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:

140[c.ii] *the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust 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, including the language of counterpart “*independent authentication*” limitations recited in claims 48, 82, and 116 if there are material differences. 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 48-50, 57, 82-84, 91, 116-118, 125, 140-142 By Russ (Ground 1)

Petitioner contends that claims 48–50, 57, 82–84, 91, 116–118, 125, 140–142 of the ’236 patent are anticipated by Russ. Pet. 18–67. Petitioner provides detailed claim charts mapping the language recited in claims 140–142 to the disclosures in Russ with citations to Dr. Wasilewski’s testimony in support. *Id.* at 21–50. Given the similarities in claim language, Petitioner addresses the other challenged claims by providing cross-citations to its argument and evidence regarding claims 140–142, with additional analyses provided for certain claims to support Petitioner’s anticipation argument. *Id.* at 51–67.

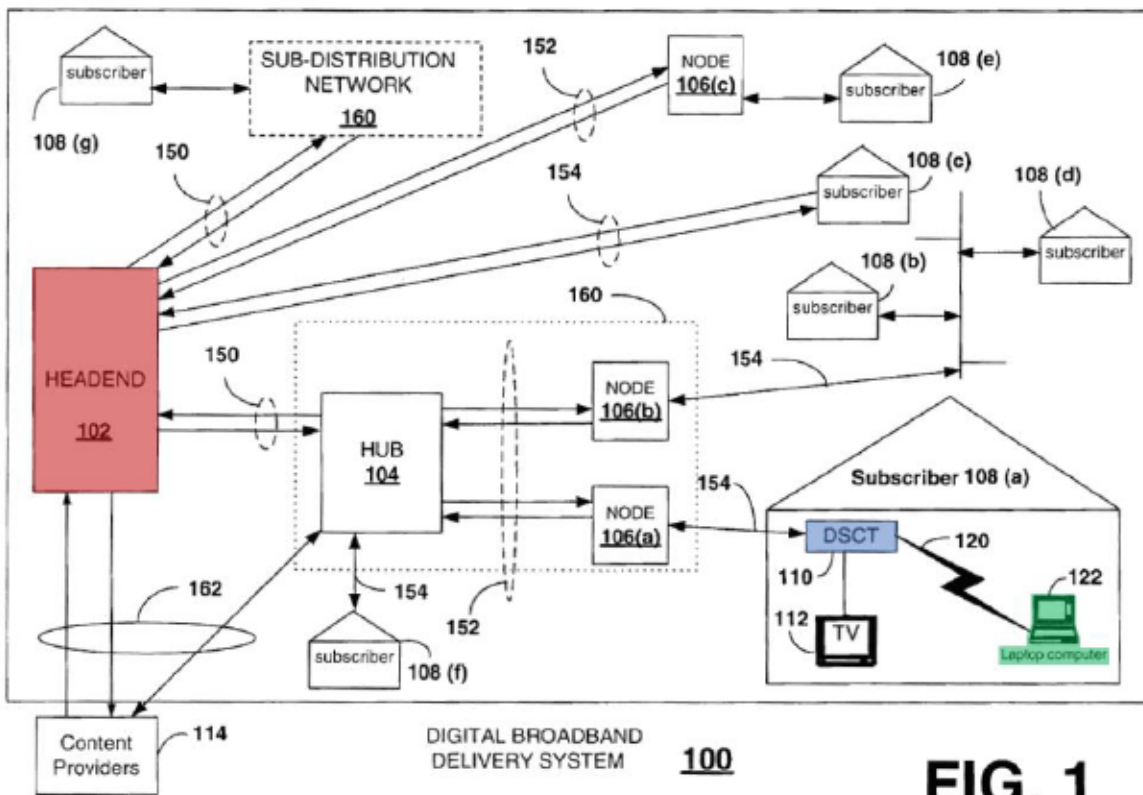
Anticipation under 35 U.S.C. § 102 requires “the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim.” *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010); *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (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 '236 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. 19 (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. *Whether Russ discloses or teaches “independent authentication”*

Petitioner maps the “*independent authentication*” limitation 140[c.ii] 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. 44–45 (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* Wasilewski Dec. Ex. 1003 ¶¶ 96 (“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; Ex. 1012 ¶ 41)); 97–99. 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. 44 (citing 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. 13–21. 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) using DTLA [Digital Transmission Licensing Authority] licensed certificates’ at all.” *Id.* at 13 (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. 44 (citing Ex. 1003 ¶¶ 94–99); *see 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” AKE key exchange and authentication of the client-receiver by the DSCT (via DTLA license certificate) and a POSA would have recognized that fact. Ex. 1003 ¶ 96 (citing Ex. 1010 ¶ 9; 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.* ¶¶ 97–99.

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 “is first brought into the local network of the DSCT,” 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, 26:39–48).

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 140[c.i].” Pet. 44 (citing Ex. 1003 ¶¶ 94–99; 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 ¶¶ 98–99. 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 “*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. 16–21. 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 16–17 (citing Ex. 1002, 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. 1002, 477–78; 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. 39, Ex. 1003 ¶ 83; 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. 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 ’236 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 ’236 patent] allows a user to receive secured content from a primary system without directly subscribing to the primary system services.” EX1002, 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 ’236 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, 4 (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.”) (emphasis added)).

Patent Owner does not analyze in detail the recited claim language or the corresponding written description, e.g., in column 8 of the ’236 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 ’236 patent prosecution history (Ex. 1002) in an attempt to distinguish Russ from the ’236 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 ’236 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

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 '236 patent. Prelim. Resp. 12–13 (citing Ex. 1002, 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. 41 (citing Ex. 1005, 7:21–8:3,

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.

10:39–47; Ex. 1003 ¶¶ 90–93). “[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. 44 (citing Ex. 1003 ¶¶ 94–99; Ex. 1005, 16:64–17:14; 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 ¶ 98. 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.

c. *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. 18–67 (citing Ex. 1003 ¶¶ 57–162). As addressed above, Patent Owner challenges Petitioner’s mapping of the “*independent authentication*” limitation, 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 48–50, 57, 82–84, 91, 116–118, 125, 140–142 of the '236 patent as anticipated by Russ.

D. Asserted Obviousness of Claims 48-50, 57, 82–84, 91, 116–118, 125, 140–142 of the '236 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. 67. 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.* at 68.

We agree with Patent Owner that Petitioner’s Ground 2 “fails to identify any embodiment of Russ, what ‘various relied-on features’ of other embodiments it attempts to combine, or any non-generic reason why it would have been obvious to combine any vague ‘various features’.” Prelim. Resp. 23; *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 48-50, 57, 82-84, 91, 116-118, 125, 140-142 of the ’236 patent as obvious over Russ.

III. CONCLUSION

For the foregoing reasons, we determine Petitioner has established a reasonable likelihood of prevailing in its challenge to the patentability of claims 48–50, 57, 82–84, 91, 116–118, 125, 140–142 of the ’236 patent as anticipated by Russ. 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.

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 48–50, 57, 82–84, 91, 116–118, 125, 140–142 of the '236 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 '236 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

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