

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU, INC.,
Petitioner,

v.

VIDEOLABS, Inc.,
Patent Owner.

IPR2024-01025
Patent 8,291,236 B2

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

EASTHOM, *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 100–109 and 111 (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 100–109 and 111 on all grounds set forth in the Petition. *See* 37 C.F.R. § 42.108(a).¹

¹ 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

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,” describes 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,

the 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 [a second] 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

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).

security system acts as a bridge because it is both an authorized client of the primary security system, from which it receives encrypted content, and a server of encrypted 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. Figure 2A, as annotated by Petitioner, follows:

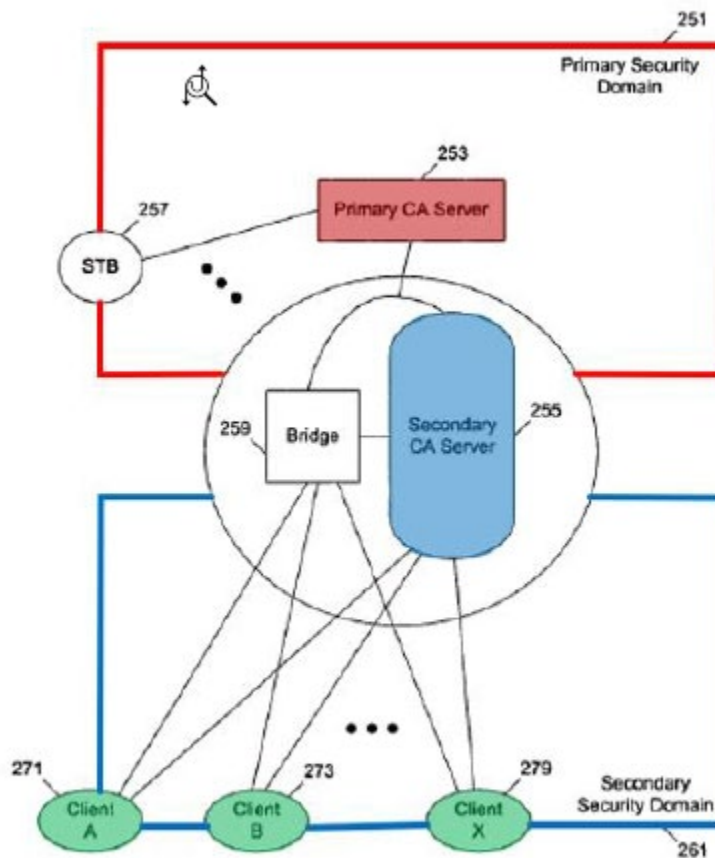


Fig. 2A

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) acts an authorized client of the primary security domain “and as a control information provider of the secondary security domain (261).” *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

Claim 100 is the sole independent claim challenged in the Petition, and follows:

100[pre]² A data processing system to process conditional access protection, the data processing system comprising:

100[a] means for receiving, at a conditional access server, security messages of a primary security system in a first security domain;

100[b] means for processing the security messages on the conditional access server; and

100[c] means for transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

100[d.i] wherein the primary security system authenticates the conditional access server as one of clients of the primary security

² For purposes of this Decision, we largely adopt Petitioner’s claim limitation reference system.

system through a first authentication process using a first root of trust and

100[d.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

100[d.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.

D. Asserted Grounds of Unpatentability

Petitioner asserts claims 100–102, 106, and 107 are unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/ Basis
100–102, 106, 107 (Ground 1)	102 ³	Russ ⁴
100–102, 106, 107 (Ground 2)	103	Russ
103–105 (Ground 3)	103	Russ, Robert ⁵
108, 109, 111 (Ground 4)	103	Russ, Eskicioglu ⁶

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

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.

⁵ US Patent No. 7,546,641 B2, issued June 9, 2009, filed Feb. 13, 2004. Ex. 1006.

⁶ US Patent No. 8,332,657 B1, issued Dec. 11, 2012, filed Mar. 15, 2000. Ex. 1007.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner describes a person of ordinary skill in the art (“POSITA”) 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. Patent Owner applies Petitioner’s proposed definition for purposes of its Preliminary Response. Prelim. Resp. 5 (citing Malek Dec. Ex. 2001 ¶ 38).⁷

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 that reflects the knowledge and experience of a POSITA.

We adopt Petitioner’s proposal for purposes of institution, which the prior

⁷ 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.

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).

1. Independent Second Authentication Process and Second Root of Trust

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.⁸ 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” “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 ’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

⁸ 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).

primary security domain.” *Id.* at 4 (citing Ex. 1001, 8:33–35). As set forth below, it is not necessary at this stage to construe the term explicitly.

2. Means-Plus-Function Terms

Petitioner asserts that the claims recite several means-plus-function limitations under 35 U.S.C. § 112 ¶ 6 and provides constructions for same.⁹ *See* 37 C.F.R. § 42.104(b)(3); Pet. 16–22 (listing means for receiving, means for processing, means for transmitting, means for decrypting, means for descrambling). Patent Owner does not address Petitioner’s claim construction as to these terms at this stage.

Under 35 U.S.C. § 112 ¶ 6,

[a]n element in a claim for a combination may be expressed as a means . . . for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

Construing a means-plus-function limitation under 35 U.S.C. § 112 ¶ 6 involves two steps: 1) identifying the claimed function and 2) identifying in the specification the corresponding structure that performs the claimed function. *Med. Instrumentation & Diagnostics Corp. v. Elekta AB*, 344 F.3d 1205, 1210 (Fed. Cir. 2003); *Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.*, 296 F.3d 1106, 1119 (Fed. Cir. 2002).

“[S]tructure disclosed in the specification” is “‘corresponding’ structure,” “only if the specification or prosecution history *clearly links or associates* that structure to the function recited in the claim.” *B. Braun Med. Inc., v. Abbott Lab’s*, 124 F.3d 1419, 1424 (Fed. Cir. 1997) (emphasis added) (“Because Braun’s

⁹ As indicated above, statutory citations are to the pre-AIA version of 35 U.S.C. § 112. *See supra* note 3.

specification does not adequately disclose the valve seat as structure that holds the disc firmly in place, Braun has failed to particularly point out and distinctly claim that particular means.”). “This duty to link or associate structure to function is the *quid pro quo* for the convenience of employing § 112, ¶ 6.” *Id.* (citing *O.I. Corp. v. Tekmar Co.*, 115 F.3d 1576, 1583 (Fed. Cir. 1997)).

Our reviewing court explains:

If the specification is not clear as to the structure that the patentee intends to correspond to the claimed function, then the patentee has not paid that price but is *rather attempting to claim in functional terms unbounded by any reference to structure* in the specification. Such is impermissible under the statute.

Med. Instrumentation & Diagnostics Corp. v. Elekta AB, 344 F.3d 1205, 1211 (Fed. Cir. 2003) (emphasis added); *see also Medtronic, Inc. v. Advanced Cardiovascular Sys., Inc.*, 248 F.3d 1303, 1313 (Fed. Cir. 2001) (finding particular structures not to be corresponding structures because “one skilled in the art would not perceive any clear link or association between these structures and the [recited] function of connecting adjacent elements together”).

After identifying the respective functions recited in claims 100, 104, 106, and 108, Petitioner proposes that the corresponding structure of “means for receiving” includes “one or more communication interfaces, a physical interface, a tuner, and statutory equivalents.” Pet. 16–17 (citing Ex. 1001, 7:53–56, 17:26–27, 17:51–18:18, 21:21, 21:33–36, 21:50–52, 21:61–62, 22:33–37; Ex. 1003 ¶¶ 53–56)).

After identifying the respective functions recited in claims 100, 104, and 108, Petitioner proposes that the corresponding structure of “means for processing” includes a microprocessor programmed with algorithms and equivalents that decrypt an EMM, decrypt an ECM to obtain a control word, and decrypt and

re-encrypt an ECM to generate a substitutive ECM, respectively. Pet. 17–18 (citing Ex. 1001, 10:36–39, 12:59–61, 13:30–34 13:44–53, 13:60–62, 14:21–24, 17:44–47, 18:48–50, 20:42–51, 21:61–63, 22:26–29, 22:41–42; Ex. 1003 ¶¶ 57–62).

After identifying the function recited in claim 101, Petitioner proposes that the corresponding structure of “means for transmitting” “includes one or more communication interfaces, a physical interface, a data network communication interface, and . . . equivalents.” Pet. 19–20 (citing Ex. 1001, 8:44–49; Ex. 1003 ¶¶ 63–66).

After identifying the function recited in claim 101, Petitioner proposes that the corresponding structure of “means for decrypting” includes “the processor” identified above, “programmed to decrypt an EMM to recover a service key, and . . . equivalents.” Pet. 20–21 (citing Ex. 1001, 10:31–34, 13:44–45, 18:4–5, 18:39–40, 21:46–48.; Ex. 1003 ¶¶ 67–70).

For institution purposes, the preliminary record supports Petitioner’s claim construction proposals for the means-plus-function terms. As indicated above, Patent Owner does not address these proposals. *See generally* Prelim. Resp.

3. Order on Claim Construction

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:

100[d.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. 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 (stating “authentication methods used by the secondary CA server in the secondary subscriber management system are independent from those used by the primary CA server”).

4. *Summary*

On the present record, we determine that no explicit construction of other 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)).

C. Asserted Anticipation of Claims 100–102, 106, and 107 by Russ (Ground 1)

Petitioner contends that Russ anticipates claims 100–102, 106, and 107. Pet. 23–61. Supported by the testimony of Dr. Wasilewski, Petitioner provides a detailed mapping of the claim elements to show how Russ anticipates the claims. *See id.*

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)).

1. Russ (Ex. 1005)

The Russ patent, titled “Apparatus For Entitling Remote Client Devices,” describes 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). Petitioner’s annotated version of Russ’s Figure 1 follows:

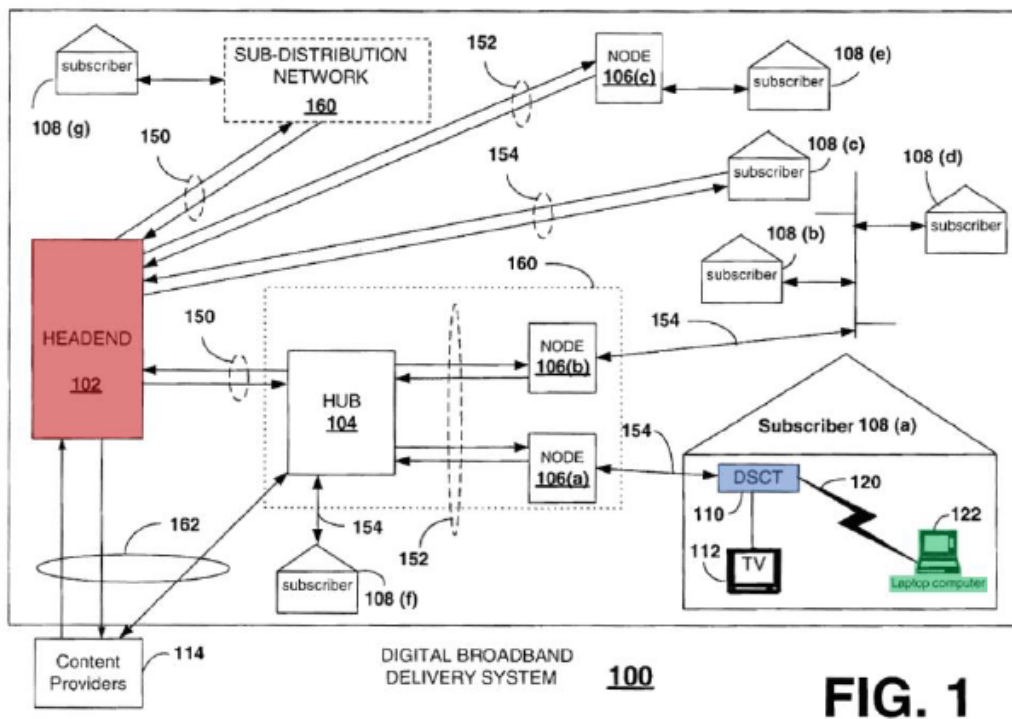


FIG. 1

Pet. 23 (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. *Id.* at 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. Ex. 1005, 17:61–18:40, 18:60–65. The DSCT and client-receiver communicate a dynamic encryption scheme when 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, including the disputed “*second root of trust*,” to Russ’s disclosure of the dynamically determined DTCP encryption protocol for communicating content to the client-receiver. Pet. 45–46 (citing Ex. 1005, 16:64–17:14). Petitioner relies on testimony by Dr. Wasilewski and cites extrinsic evidence to support its assertion that the disclosed DTCP encryption protocol requires a separate authentication and key exchange between the DTSC and client-receiver, “thereby explaining what the phrase [DTCP encryption protocol] would have meant to one skilled in the art.” *See In re Baxter*, 952 F.2d at 390; Pet. 45–46 (citing Ex. 1003 ¶¶ 126–131; Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107, 139–143); Ex. 1003 ¶ 128 (“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)). Petitioner asserts the extrinsic evidence demonstrates a person of ordinary skill in the art “would have recognized that DTCP protocols include

authentication and key and certificate exchange procedures that ensure communications are protected.” *Id.* at 46 (citing Ex. 1010 ¶ 9; Ex. 1011 ¶¶ 53, 107, 139–143, Fig. 17; Ex. 1003 ¶¶ 126–131).

Patent Owner argues that Petitioner does not 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) using ‘DTLA [Digital Transmission Licensing Authority] licensed certificates’ at all.” *Id.* at 13–14 (citing 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 showing sufficiently that Russ discloses the second root of trust to a person of ordinary skill in the art, who “would have recognized that [Russ’s] DTCP protocols include authentication and key and certificate exchange procedures.” Pet. 46 (citing Ex. 1003 ¶¶ 126–131); *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 ¶ 128 (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.* ¶¶ 130–131 (emphasis added).

At this stage, Patent Owner disputes Petitioner’s evidence that a POSITA 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” in an attempt 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 showing that DTCP encryption requires an AKE key exchange and a DTLA license certificate. *Id.* (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, 26:29–48).

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 100[d.i].” Pet. 45–46 (citing Ex. 1003 ¶¶ 126–131; 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 ¶¶ 130–131. 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 argues that 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. 16–22. 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. 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. *See* Ex. 1002, 477–78; Prelim. Resp. 20–21 (citing Ex. 1002, 477). 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. 20–21.

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.” Prelim. Resp. 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 (first quote quoting Ex. 1005, 25:17–22). Patent Owner's argument, however, is not consistent with Russ, which states as follows:

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 (emphases added). Russ makes clear that headend determination of the encryption scheme for the client-receiver is not a requirement, but rather an alternative to DSCT control via dynamic encryption determination with the client-receiver.¹⁰

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 Applicant distinguished during prosecution of the '236 patent.

¹⁰ 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. Ex. 1005, 20:11–47.

Prelim. Resp. 12–13 (citing Ex. 1002, 478; quoting Ex. 1005, 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. 44 (citing Ex. 1005, 7:21–8:3, 10:39–47; Ex. 1003 ¶¶ 122–125). “[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. 45–46 (citing Ex. 1003 ¶¶ 126–131; 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

¶ 130. 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. 22–61 (citing Ex. 1003 ¶¶ 79–179). 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 challenged claims 100–102, 106, and 107. 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 100–102, 106, and 107 of the ’236 patent as anticipated by Russ.

D. Asserted Obviousness, Grounds 2–4

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)). Resolving obviousness involves 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)).

A petition for *inter partes* review also 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.*

1. Asserted Obviousness of Claims 100–102, 106, and 107 over Russ (Ground 2)

As Patent Owner argues, Petitioner presents a vague “catch-all” obviousness argument based on Russ (Prelim. Resp. 23), arguing that “Russ further teaches that its disclosed features are combinable, and a POSA would have thus found the claims obvious” (Pet. 62). Rather than providing a particularized showing that demonstrates how specific features and embodiments disclosed in Russ are combinable, Petitioner relies instead on generic statements that “various examples and embodiments disclosed in Russ are directly related to each other,” contending that a person of ordinary skill in the art 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 62.

As Patent Owner argues, 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 also 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 that Petitioner fails to demonstrate a reasonable likelihood it would prevail in showing the unpatentability of claims 100–102, 106, and 107 as obvious over Russ.

2. *Asserted Obviousness of Claims 103–105 over Russ and Robert (Ground 3)*

i. *Robert (Ex. 1006)*

Robert relates 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, 1:50–2:19. Unifying includes translating aspects of CA schemes into a DRM-type content license. *See id.* at Fig. 5. As background, 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 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:

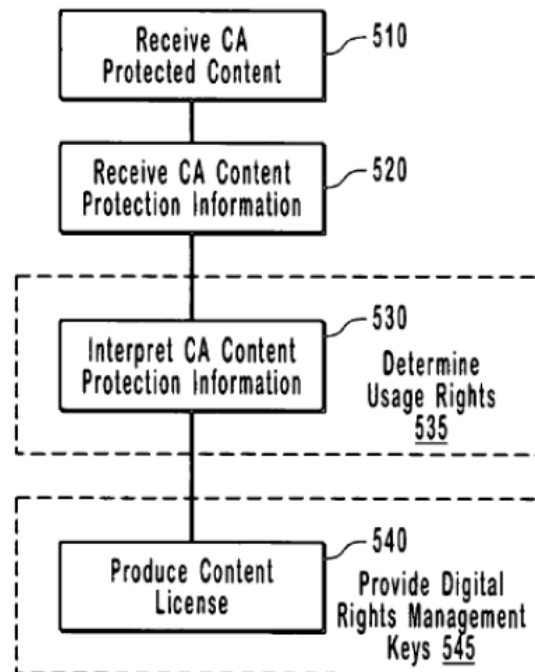


Fig. 5

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.

ii. *Obviousness, Russ and Robert*

Petitioner contends that claims 103–105 would have been obvious over Russ in view of Robert. Pet. 63–74.

Claim 103 recites “[t]he data processing system of claim 102, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.” As indicated above in summarizing Petitioner’s anticipation showing, Petitioner shows sufficiently that Russ anticipates claim 102, which recites “[t]he data processing system of claim 100, wherein the access controlled data is protected using a digital rights management system.” See Pet. 50 (showing, *inter alia*, that Russ’s DTCP system is a known digital rights management system (citing Ex. 1013 ¶ 14) (“Examples of traditional digital rights management authentication methods include . . . DTCP.”); Ex. 1003 ¶¶ 149–151)).

Referring to its anticipation showing for claim 100, Petitioner contends that Russ discloses a system in which DSCT 110 provides service instances and entitlements via an EMM to client-receiver 122. See Pet. 69 (citing Ex. 1005, 16:64–17:14, 17:61–18:66, 21:11–21, 24:1–24, 21:22–65). Petitioner explains that DSCT 110 manages its own local network at a subscriber location and serves client-receiver 122 with service instances and entitlements communicated with a dynamic encryption scheme for use between DSCT 110 and client-receiver 122 only. See *id.* at 65. Petitioner also explains that “Russ discloses that DSCT 110 receives an entitlement for a service instance in an EMM [from head-end 102], then processes the EMM and provides the entitlement to client-receiver 122.” *Id.* at 66 (citing Ex. 1005, 18:60–19:6). However, according to Petitioner, Russ “leaves to the POSA specific implementation details regarding entitlements or usage rights for the myriad of encryption schemes that may be selected for

communications between DSCT 110 and client-receiver 122, like DTCP or CPRM DRM schemes.” *Id.* at 66 (citing Ex. 1005, 16:64–17:14).

Contending that Russ does not disclose or teach the specific implementation details, Petitioner asserts that “Robert teaches interpreting content protection information for the CA content to determine usage rights, producing a content license according to those usage rights, and then providing DRM keys to a destination device with those rights.” Pet. 66 (citing Ex. 1006, 12:16–26). Petitioner further asserts that “[b]y interpreting and deriving rights from the original protection information, the system ‘maintain[s] security of the content and any associated protection content information (e.g., usage rights, access conditions, encryption keys, etc.).’” *Id.* (quoting Ex. 1006, 4:50–65, 6:19–26). Therefore, Petitioner contends that it would have been obvious to modify Russ’s scheme using Robert’s teaching to “provide rights to services instances, transmitted to client-receiver 122 via DTCP protocols, that are derived from the entitlement received at DSCT 110, so that rights are not lost or evaded between headend 102, DSCT 110, and . . . at the subscriber location’s client-receiver 122.” *Id.* at 66–67 (citing Ex. 1003 ¶ 190).

Petitioner also explains as follows:

In addition to Russ’s disclosures that entitlements received via EMM at DSCT 110 are processed and provided to client receiver 122, whose communications are protected by the dynamically determined encryption scheme such as DTCP as discussed in at least claims 100[c.ii]–[c.iii], Robert teaches *translating content from one content protection scheme to another by interpreting and transcribing content protection information into a usage rights license*. . . . A POSA would have been motivated to derive client-receiver 122’s rights to service

instances by interpreting received EMMs, as taught by Robert, as discussed in §VII.C.2.

Pet. 69–70 (citing Ex. 1005, 12:8–26; Ex. 1003 ¶¶ 186–189) (emphasis added). In other words, Petitioner’s showing includes modifying Russ’s DTCP encryption scheme, which employs a usage rights license (certificate), by implementing similar usage rights license techniques and interpreting EMMs according to Robert’s teachings. *See* Ex. 1003 ¶ 129 (testifying that “[t]he DTCP certificate identifies a DTCP device and contains verifiable proof that the device is licensed to operate as a DTCP device” and “[l]icensing in this case is performed by a trusted licensing authority, such as the Digital Transmission Licensing Administrator (‘DTLA’), which is the licensing organization of DTCP” (citing Ex. 1011 ¶¶ 53, 107)).

Claim 104 recites

104[pre] [t]he data processing system of claim 102, further comprising **104[a]** means for receiving, at the conditional access server, an entitlement control message of the primary security system; and **104[b]** means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system; **104[c]** wherein access controlled data comprises the control word.

Petitioner contends that “Robert teaches that access controlled data transmitted to a destination device includes the control words for decrypting content protected by DRM.” Pet. 67 (citing Ex. 1006, 9:53–10:4). “By providing the control words, . . . the destination device can use a DRM license to decrypt CA-protected content.” *Id.* (citing Ex. 1006, 9:66–10:4). Petitioner also contends that it would have been obvious “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 67–68. 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 68 (citing Ex. 1005, 19:50–59; Ex. 1003 ¶¶ 191).

Petitioner further argues that “[a] POSA would have had a reasonable expectation of success implementing Russ’s system by deriving rights from EMMs and including decrypted ECM [entitlement control message] information [(Ex. 1005, 13:20–22)], including control words, as access controlled data,” where “both Russ and Robert explain that content protection protocols and encryption schemes are well-known processes.” Pet. 68 (citing Ex. 1005, 17:7–14; Ex. 1006, 5:10–11).¹¹

Similar to its showing for claims 103 and 104, for claim 105 Petitioner sets forth a detailed showing including sufficient reasons to combine Russ and Robert with a reasonable expectation of success. *See* Pet. 71–74.

For purposes of institution, we determine the preliminary record supports Petitioner’s showing that claims 103–105 would have been obvious over Russ and Robert. *See* Pet. 63–74.

Patent Owner relies on its unavailing arguments addressed above with respect to anticipation in Ground 1, and does not address the merits of Petitioner’s

¹¹ “Typically, ECMs are transmitted without being encrypted so that the DSCTs do not have to spend time to decrypting the content of the ECM before generating the control word.” Ex. 1005, 13:23–26 (“However, the ECMs include an authentication token that is used for authenticating the message content and limiting access thereto . . .”).

arguments and evidence in support of the asserted obviousness of claims 103–105. Prelim. Resp. 22–23.

Based on a review of the record, we determine that Petitioner demonstrates a reasonable likelihood of prevailing in showing that claims 103–105 would have been obvious.

3. *Asserted Obviousness of Claims 108, 109, and 111 over Russ and Eskicioglu*

i. *Eskicioglu (Ex. 1007)*

Eskicioglu relates to a copy protection system that provides security during transmission and storage of content. Ex. 1007, code (57), 1:15–20. Eskicioglu discloses local protection within a home network by rebundling keys required for descrambling content, from an ECM into a local ECM (“LECM”) protected by a unique key. *Id.* at 2:1–40.

Figure 4 of Eskicioglu follows:

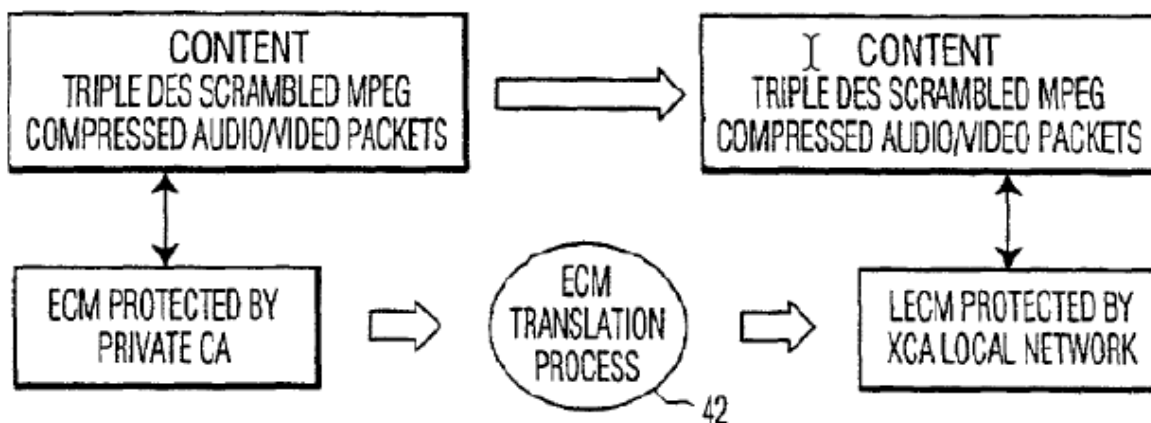


FIG. 4

Figure 4 illustrates an ECM undergoing ECM translation process 42, which rebundles “the keys required for descrambling . . . into a new ECM which is

protected by a local public key associated with the access device (i.e., LECM).”
Id. at 8:4–7.

ii. *Obviousness, Russ and Eskicioglu*

Petitioner contends that claims 108, 109, and 111 would have been obvious over Russ in view of Robert. Pet. 75–84.

Claim 108 recites “**108[pre]** [t]he data processing system of claim 100, further comprising, **108[a]** means for receiving, at the conditional access server, an entitlement control message of the primary security system; and **108[b]** means for processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message; wherein the access controlled data comprises the substitutive entitlement control message.”

Petitioner refers to its showing for claim 100 to address recitation 108[pre]. Pet. 79. Petitioner reads limitation 108[a]’s “means for receiving . . . an entitlement control message” onto Russ’s input-port 302 or tuner 304 at DSCT 110, which receives encrypted service instances or programs from headend 102 in the form of encrypted content of a multi-transport stream or of encrypted service instances (encrypted with control words or other scrambling techniques) including within an ECM. *See id.* at 79, 51 (citing Ex. 1005, 5:52–6:7, 7:56–58, 13:3–5, 12:47–13:11, 13:14–34, 13:53–56, 15:1–6 Figs. 2–3; Ex. 1003 ¶¶ 15:3–15). Petitioner notes that Russ teaches that “[e]ntitled’ DSCTs 110 are allowed to use the decryption information to decrypt encrypted content.” *Id.* at 53 (quoting Ex. 1005, 13:1–11).

Addressing limitation 108[b], Petitioner contends that “Russ discloses that client-receiver 122 decrypts service instances by generating control words and does not explicitly explain the origin of those control words, but explains that

DSCT 110 and client-receiver 122 communicate with negotiated protocols and encryption in one of any number of schemes known to POSAs.” Pet. 77 (citing Ex. 1005, 16:64–17:60, 20:12–17, 26:16–28, 26:34–37, 26:54–67). Petitioner also contends that

Eskicioglu teaches one variety, extended conditional access (“XCA”), for protecting received CA content in local networks. . . . In a system where CA content is received by an access device and destined for consumption at a presentation device, ECMs associated with the CA content and protected by a service providers’ keys, are rebundled into LECMs protected by a local public key.

Id. (citing Ex. 1007, 1:16–20, 2:1–40, 2:65–3:11, 3:50–4:15, 7:41–53, 8:4–18).

Therefore, where Russ teaches using known encryption schemes for communication between DSCT 110 and client-receiver 122 including use of ECMs, Petitioner contends that it would have been obvious “to generate and transmit a substitutive ECM (or LECM) with a control word encrypted with DSCT 110’s key, as taught by Eskicioglu, to protect content in the local network and to ensure that the content is protected and not accessed outside the local network.”

Pet. 76 (citing Ex. 1007, 8:10–18). Petitioner further explains that

[a]s Russ discloses that the service instance may not need to be decrypted first by DSCT 110 . . . , use of the new LECM with the same service instance received from headend 102 would have saved time and resources at DSCT 110 while further substituting the primary security domain provided by headend 102 (via the original ECM) with the secondary security domain provided by DSCT 110 (via the LECM).

Id. at 78 (citing Ex. 1005, 19:50–59; Ex. 1003 ¶ 206).

Claim 109 recites “[t]he data processing system of claim 108,, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.” Petitioner contends that “Eskicioglu discloses that the substitutive entitlement control message has a control word (e.g., the

LECM is a rebundled ECM, including control words) encrypted using a key of the conditional access server (e.g., the LECM is encrypted with the public key associated with the access device).” Pet. 83 (emphasis omitted). According to Petitioner, “Eskicioglu discloses that the LECM includes control words (or equivalent keys) for descrambling content.” *Id.* (citing Ex. 1007, 2:3–7, 7:41–53). Petitioner also explains that “[t]he LECM contents are encrypted with a unique key associated with the conditional access server—i.e., associated with a ‘first’/‘access’ device 14 that receives the content and ECM and rebundles the ECM into the LECM.” *Id.* (citing Ex. 1007, 2:3–7, 7:41–46, 8:19–30; Ex. 1003 ¶¶ 226–228).

In addition to the reasons to combine noted above for claim 108 (which also applies to claim 109), Petitioner asserts that

such implementation would have been, at least, the application of a known technique (e.g., Eskicioglu’s teachings of XCA protocols) to a known system ready for improvement (e.g., Russ’s disclosure of DSCT 110 and client receiver 122 negotiating communications via any protocols known to POSAs) to yield predictable results (e.g., maintaining security of communicated data to client devices using LECMs).

Pet. 78–79 (citing *KSR*, 550 U.S. at 415–421).

Claim 111 recites “[t]he data processing system of claim 109, wherein the entitlement control message and the substitutive entitlement control message have a same control word.” Referring to its showing for claims 108 and 109, Petitioner contends that Eskicioglu’s ECM and LECM have the same control word. Pet. 84 (citing Ex. 1007, 1:66–2:10, 7:41–53, 8:4–12; Ex. 1003 ¶¶ 218–220).

For purposes of institution, we determine the preliminary record supports Petitioner’s showing that claims 108, 109, and 111 would have been obvious over Russ and Eskicioglu. *See* Pet. 75–83.

Patent Owner relies on its unavailing arguments addressed above with respect to anticipation in Ground 1, and does not address the merits of Petitioner's arguments and evidence in support of the asserted obviousness of claims 108, 109, and 111. Prelim. Resp. 22–23.

Based on a review of the record, we determine that Petitioner demonstrates a reasonable likelihood of prevailing in showing that claims 108, 109 and 111 would have been obvious.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner establishes a reasonable likelihood of prevailing in showing the unpatentability of the challenged claims. Therefore, we institute *inter partes* review of the challenged claims. 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 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.

Case IPR2024-01025

Patent 8,291,236 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 DeMORY LLP

jtice@bdiplaw.com

ahand@bdiplaw.com