UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner

Case IPR2024-01025
U.S. Patent 8,291,236

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

Page

I. Introduction.....1

II. The ’236 Patent.....3

A. Person of Ordinary Skill in the Art (POSITA) 5

III. The Petition fails to demonstrate a reasonable likelihood of Success as to any Challenged Claim. 6

A. The Claimed Solution of the ’236 Patent.....7

B. Russ’s Different Problem and Different Proposed Solution.....9

C. The Petition Fails to Demonstrate that Russ Discloses a “Second Root of Trust.” 13

D. The Petition Fails to Demonstrate that Russ Discloses “a Second Root of Trust Which is Independent of and Different Than the First Root of Trust.” 16

E. Grounds 2-4 Cannot Demonstrate any Reasonable Likelihood of Success. 22

IV. The Board Should Deny Institution for Violating the “Particularity” Requirement.....22

V. Conclusion 24

TABLE OF AUTHORITIES

Page(s)

Cases

Adaptics Ltd. v. Perfect Co.,
IPR2018-01596 (P.T.A.B. Mar. 6, 2019) 22

Harmonic Inc. v. Avid Tech., Inc.,
815 F.3d 1356 (Fed. Cir. 2016) 23

Statutes

35 U.S.C. § 312(a)(3) 23

35 U.S.C. § 314(a) 2

PATENT OWNER'S APPENDIX OF EXHIBITS

Exhibit	Description
EX2001	Declaration of Dr. Sam Malek
EX2002	Curriculum Vitae of Dr. Sam Malek
EX2003	Company Overview, Digital Keystone (https://web.archive.org/web/20031206063740/http://www.digitalkeystone.com/profile/mission.htm)

I. INTRODUCTION

The Board should deny institution of *inter partes* review of U.S. Patent No. 8,291,236 (the "'236 patent") because the Petition fails to demonstrate any reasonable likelihood of success for any challenged claim. For each challenged independent claim, Petitioner relies only on the Russ reference. In ground 1, Petitioner alleges that Russ anticipates each independent claim. That is incorrect: Russ teaches a system that includes the limitations that the '236 inventors sought to overcome, and therefore does not disclose each element of the challenged claims.

The inventors of the '236 patent disclosed a system in which devices of one security domain could receive content from an independent domain via a conditional access (CA) server that acts as a "bridge" between the two domains. The conditional access server can independently authenticate and provide content to devices that are located only within the second security domain. The conditional access server can also act as a client to receive content in a first domain and then provide it to its clients in the second security domain. This allowed "a user to receive content from a primary system without directly subscribing to the primary system services." EX1002, 381.

The Russ reference is the antithesis of the inventions described and claimed in the '236 patent. Russ describes a single subscriber system in which one entity (headend 102, an "operator") controls the entire network, i.e., Russ's alleged first

CA server. Russ's alleged second CA server therefore cannot authenticate any of the subscriber's devices without the direction and control of the alleged first CA server—there is ***no independence*** as required by the claims.

Realizing this, Petitioner argues anticipation by inventing disclosure that is not present in Russ. This alone renders the Petition meritless. Regardless, Russ fails to teach or suggest any authentication using a "second root of trust" that is independent from a "first root of trust," because Russ includes a single entity that controls the entire system, and any operation of the system is dependent on that entity and its root of trust.

A separate deficiency of the Petition is its failure to meet the particularity requirement for ground 2. There, Petitioner argues that Russ instead renders obvious the challenged independent claims. This argument not only highlights the failures of Russ for ground 1 but presents another reason why institution should be denied: Petitioner's explanation for ground 2—spanning less than a page—falls far short of the particularity requirement of Section 314(a). The proposed ground 2 is a prohibited "catch-all" ground, arguing that it would have been obvious to combine any feature of any of the discrete embodiments of Russ with all other features of all other discrete embodiments. Pet., 62. The Petition fails to identify any embodiment of Russ or any feature(s) of other embodiments that it seeks to combine. *Id.* Instead, Petitioner relies on generic disclosures of Russ that changes or modifications can be

made to argue that anything in Russ can be combined with anything else. Petitioner's catch-all ground, which leaves the door open to present obviousness theories for the first time in Reply, should be rejected for failing to comply with the particularity requirement.

II. THE '236 PATENT

U.S. Patent No. 8,291,236 (the "'236 patent"), titled "Methods and Apparatuses for Secondary Conditional Access Server," issued on October 16, 2012. EX1001, Face Page.

The original assignee of the challenged patent is Digital Keystone, Inc. ("Digital Keystone"), a Silicon Valley based video technology company. Digital Keystone develops digital entertainment technologies, including security software for video applications. In the early 2000s, when the inventions of the challenged patent were in development, Digital Keystone was creating world-first digital entertainment solutions that bridged the personal computer, consumer electronics and content industries. Next generation digital cable TVs, PC-based entertainment systems and media distribution networks were powered by Digital Keystone hardware and software technologies. And Digital Keystone was also licensing its industry-leading security technology to TV broadcasters, consumer electronics manufacturers, developers of digital home components, and chip manufacturers. EX2003. In partnership with Microsoft and CableLabs, Digital Keystone developed

the world's first secure Pay TV bridge, which was demonstrated by Bill Gates in his keynote speech during the 2006 Consumer Electronics Show. The challenged patent discloses and claims a bridge, such as the one touted. Digital Keystone was at the forefront of enabling secure content access throughout the entire home.

As discussed in more detail in Section III.A, the '236 patent teaches bridging two separate security domains using a "conditional access server." EX1001, Abstract. For example, a first security domain could be "a broadcast CA system," such as a cable television broadcast system. *See id.*, 2:61-67, Fig. 3. A second security domain could be "a digital rights management system," such as used for streaming content over the Internet, or a separate CA system such as satellite television. *Id.*

Before the invention of the '236 patent, each device displaying content from one of these systems had to be subscribed to and authenticated by the system. EX1002, 381. However, with the proliferation of differing devices and differing security domains, it became difficult for a device to receive content from various security domains, as devices could not be authenticated by each of the everchanging and evolving domains. *See*, *e.g.*, EX1001, 9:60-64 (describing needing two separate set-top boxes for two separate satellite TV networks). The inventors developed a "secondary conditional access server" that could independently verify devices. *See*, *e.g.*, EX1001, 8:3-38, claim 130. The secondary access server could then provide

content from various security domains to the verified device, without the devices having to be verified within each security domain. *Id.*; *see also* EX1002, 381.

A. Person of Ordinary Skill in the Art (POSITA)

Petitioner alleges that a POSITA "would have had 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.

For purposes of this POPR, Patent Owner and its expert apply Petitioner's proposed definition, as the Petition fails under any definition of a POSITA. *See* Malek Dec., ¶ 38.

Patent Owner notes that Petitioner has not shown that its expert, Dr. Wasilewski, qualifies as a POSITA under its definition. Petitioner has not shown that Dr. Wasilewski holds a "bachelor's degree in computer science, electrical engineer, or a related field." Instead, Dr. Wasilewski received a Bachelor of Arts degree in physics and a Ph.D. in astronomy. EX1004, 3.

This is contrasted with Patent Owner's Expert, Dr. Sam Malek, who has a bachelor's degree in Information and Computer Science as well as doctorate and master's degrees in Computer Science, in addition to being a Full Professor in the School of Information and Computer Sciences at the University of California, Irvine

and having decades of experience in the precise technical field at issue here. *See* Malek Dec., ¶¶ 5-18.

III. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS AS TO ANY CHALLENGED CLAIM.

The Petition challenges one independent claim of the ’236 patent, claim 100. And Petitioner relies only on Russ as purportedly teaching or suggesting that claim. *See* Pet., 9 (Grounds 1 and 2) (Petitioner adds Robert and Eskicioglu in Grounds 3 and 4 only in an attempt to cure Russ’s deficiencies with respect to dependent claims). Russ, however, discloses a different system aimed at a different problem. As such, it fails to teach or suggest all elements of the independent claim, including the following limitation:

> “a second root of trust which is independent of and different than the first root of trust.”

EX1001, claim 100.

Petitioner’s theories for this element fail for two reasons. First, Petitioner fails to demonstrate that Russ discloses “a second root of trust” at all. And, even if Russ did, the Petition also fails to demonstrate that Russ discloses a second root of trust “which is ***independent*** of and different than the first root of trust.” Petitioner instead focuses on the “different” requirement of the claim and, other than simply reciting claim language, fails to address entirely why its alleged “second root of trust” is

independent of its "first root of trust." Petitioner's failures are even more problematic here because the "independent" requirement was used in prosecution as a basis to overcome prior art. There is good reason why Petitioner fails to address this requirement: Russ is like the prior art discussed and overcome during prosecution that does not have two independent roots of trust. Russ fails for that same reason.

Neither Robert nor Eskicioglu cure the deficiencies of Russ for these elements, and Petitioner makes no argument to the contrary. As such, the Petition fails to demonstrate any reasonable likelihood of success for any challenged claim.

A. The Claimed Solution of the '236 Patent

The '236 patent is related to conditional access (CA), "a technique for limiting the access of content (e.g., audiovisual works such as movies) to authorized users." EX1001, 1:13-15. As the inventors described, the inventions of the '236 patent allow for "bridging between two security systems so that a secondary security system can securely present to a user a content previously secured by a primary security system. The … bridging process connects two independent authentication processes." EX1002, 478. As an example, the first security system can include a first conditional access (CA) server for clients authenticated using a first authentication process, and the second security system can include a second CA server for different clients authenticated using an independent, second authentication process. *Id.*

The inventors described that "[i]n the prior art approaches, a client of a secondary CA server would need to subscribe to the primary CA server in order to receive services from the primary CA server." *Id.* at 479. The inventions of the '236 patent, however, provide the advantages of "allow[ing] a user to receive secured content from a primary system without directly subscribing to the primary system services." *Id.* Instead, after independently authorizing its clients, the secondary CA server may receive data from the first security domain and provide it to its clients, without the clients needing to subscribe to the first security domain or be authenticated within the first security domain. *Id.* This allows for "two security systems having two independent authentication processes." *Id.* During prosecution, the inventors also clarified the claims by requiring that the two authentication processes "use two different roots of trust that are independent." *Id.* at 477.

With this explanation, the inventors distinguished prior art references presented by the Examiner. For example, the inventors distinguished references presented by the Examiner that disclosed only "a single DRM system." *Id.* The Simelius reference, for example, disclosed a parent client and a child client with the single DRM system. *Id.* In Simelius, "[t]he parent client must verify that the child client public key is chaining to the root of trust of the content server." *Id.* As the inventors explained, this did not disclose two independent authentication processes

using two independent roots of trust, but taught that a parent client could "act as authentication proxy" for child clients in the same DRM system. *Id.* at 478.

B. Russ's Different Problem and Different Proposed Solution

U.S. Patent No. 6,748,080 to Russ et al. (EX1005, "Russ") is titled "Apparatus for Entitling Remote Client Devices." While the '236 patent is directed to two separate security domains, such as two different "subscriber management systems" (EX1001, 8:12-21), Russ, like the art discussed during prosecution, is directed to a single "subscriber network" system wherein content access and authorization is controlled by a single administrative component, Russ's "headend 102." EX1005, claim 1); Malek Dec., ¶ 44. Russ describes a conventional broadband system, such as a cable or satellite television system. EX1005, 1:14-16; *see also id.*, 3:11-12 (embodiments described "in a subscriber television network."). Russ's Figure 1 illustrates a subscriber network. As shown, the network includes a "Headend 102" and a digital subscriber communications terminal (DSCT) connected to a subscriber's devices (TV and laptop) with a wired and wireless connection. *Id.*, Fig. 1; Malek Dec., ¶ 44. As explained in more detail below, the headend 102 provides content to subscriber devices within the subscriber network. *See*, *e.g.*, EX1005, 1:15-19; Malek Dec., ¶¶ 44-45. The headend acts as an operator for the system—managing encryption of communications between devices in the network and which

devices in the network are authenticated for receiving content. EX1005, 25:17-22; Malek Dec., ¶¶ 44-48.

Like conventional systems, Russ's system included, at "a subscriber location, a digital subscriber communications terminal (DSCT)," such as a set-top box. EX1005, 1:36-44. The DSCT was typically connected to a television or other device via wired connection such that they receive content "from the subscriber network." *Id.* Russ recognized that, as portable devices were coming available, it could be "desirable to couple subscriber device to the DSCT using wireless communication." *Id.*, 1:46-64. This would allow "the subscriber to easily move his or her portable computing device … while remaining connected to the subscriber network through the subscriber's DSCT." *Id.*

Russ recognized that connecting wirelessly to the DSCT "introduce[s] security and control concerns for the operators of the subscriber network system." Russ stated that "communication signals over wireless links are more readily intercepted than signals over wired links, wireless communication links are inherently less secure." *Id.*, 2:63-66. Russ therefore proposed encrypting information communicated from the DSCT to a wireless subscriber device. *See, e.g.*, *id.*, 25:19-25. As Russ describes, a "headend 102 determines the encryption scheme used to communicate information between the DSCT 110 and the client-receiver 122." *Id.*, 25:17-22. Russ also disclosed the headend dictating the encryption scheme for

communication of content between the DSCT 110 and client-receiver 122 through use of tables. Malek. Dec., ¶ 46. Russ discloses that "[s]ystem tables are prepared by the control system 232 [of headend 102] and transmitted to the DSCT 110." EX1005, 14:50-55; *id.*, Fig. 2 (control system 232 is part of headend 102). The DSCT stores the tables in its memory. *Id.*, 14:50-55.

Once the DSCT receives a message from a client-receiver 122, the client-receiver is identified by the headend, either using the tables provided by the headend or by forwarding the message to the headend. The headend, via its own processor or the tables "identifies[] a client-receiver" and, based on the device type of the client-receiver, determines what encryption to apply. *Id.*, 16:43-50, 16:55-63; *see also id.*, 17:24-29 (the DSCT uses the tables from the headend to identify an encryption scheme). In any event, the headend controls encryption. *See also id.*, 25:17-19 ("The system controller 232 can also send an EMM to the DSCT 110 instructing the processor 312 to no longer determine the encryption scheme for the client-receiver 122.").

Moreover, Russ teaches that the operator of the subscriber network "wants the capability to control the type of devices that receive information from the DSCT or the type of content that the device receives." *Id.*, 2:66-3:2; *see also id.*, 2:55-60 ("The operator of a subscriber network system desires the ability to entitle (or disentitle) subscriber devices, i.e., to enable (or prevent) the subscriber devices from accessing

communication transmitted over a local area network, which may include wired communication links, wireless communication links, or a combination thereof."). As Russ wants the operator of the subscriber network to perform this control, it discloses the headend 102 performing the control. The control system of the headend, for example, "allows the DBDS [digital broadband delivery system] system operator to control and monitor the functions and performance of the DBDS" including "conditional access for the content distributed to subscribers." *Id.*, 10:25-34. The operator, headend 102 includes a "conditional access authority (CAA)" for controlling content distribution to devices. "The DSCT 110 receives entitlements for the service instances from the Entitlement Generator 236 of the control system 232." *Id.*, 15:43-45. Moreover, "[t]he system controller 232 can also block services or service instances. In that case, the system controller 232 sends messages and/or tables to the DSCT 110 that instruct the DSCT 110 which types of client-receiver devices can receive which type of service or service instance." *Id.*, 24:52-56. Further, "the system controller 232 can send an EMM 800 to the AEMM 720 that suspends the entitlements of the client-receiver 122 to service instances. The system controller 232 can send an entitlement suspension EMM that suspends the entitlement of a specific client-receiver 122 coupled to the DSCT 110 or all client-receivers coupled to the DSCT 110. The system controller 232 may send an entitlement suspension EMM based upon the hardware type of the client-receiver 122." *Id.*, 24:66-25:7.

As is Russ's stated purpose, the headend of the subscriber network controls (1) an initial connection, (2) conditional access authority, and (3) encryption schemes for the client-receivers. *See id.*, 2:55-3:10. That is, while a DSCT in a subscriber's home may pass content to a client-receiver of the subscriber, the network operator, via the headend, controls what content can be provided to which device and how that content is delivered. The DSCT simply "acts as a proxy" at the behest of the headend. *See id.*, 19:24-26.

However, as discussed during prosecution of the '236 patent, a mere proxy fails to teach or suggest the challenged claims. *See* EX1002, 478. Russ's DSCT and client-receiver are in the subscriber network and controlled by the same headend. Like the references discussed in prosecution, Russ fails to teach "a second root of trust which is ***independent*** of and different than the first root of trust," as required by all challenged claims. Reinforcing this failure, the Petition further fails to demonstrate that Russ discloses any "second root of trust" at all.

C. The Petition Fails to Demonstrate that Russ Discloses a "Second Root of Trust."

Petitioner cannot demonstrate that Russ teaches a "second root of trust," as required by all challenged claims. EX1001, claim 100. For this requirement, Petitioner relies on "communication between DSCT 110 and client-receiver 122" using an "Authentication and Key Exchange (AKE) using DTLA licensed

certificates." Pet., 45-46. The problem with Petitioner's theory, however, is that Russ does not mention an "Authentication and Key Exchange" or "DTLA licensed certificates" at all. Malek Dec., ¶ 50. In fact, Russ explicitly teaches a different manner of exchanging keys. *Id.*, ¶¶ 50-54. As such, Petitioner's anticipation argument for ground 1 fails.

By way of background, communications between devices can involve separate concepts of authentication and confidentiality. Malek Dec., ¶ 51. As explained by Dr. Malek in more detail, authentication is used to verify that a device is who or what it claims to be. Confidentiality, on the other hand, is the principle of keeping information private. Confidentiality is primarily achieved through encryption. *Id.* Indeed, Petitioner's Exhibit 1012 explains that these concepts are distinct: as shown there, authentication occurs prior to transmission of encoded content. EX1012, ¶ 41. A device may be authenticated without providing any encrypted communications. *Id.* Likewise, encrypted information may be transmitted to a device without authentication. *Id.*

For its "second authentication" theory, Petitioner relies on one paragraph in Russ, relating to confidentiality, with no discussion of authentication. Pet., 46 (citing EX1005, 16:64-17:14). Here, Russ only discloses that content transmitted to the client-receiver 122 may be "transmitted so as to protect the privacy of the communication." EX1005, 16:65-67. Russ then provides a list of "encryption

scheme[s]," including Digital Transmission Content Protection (DTCP). *Id.*, 17:7-14. In Russ, after a device is authenticated, content can then be provided to it using an encryption scheme, such as DTCP or other "encryption schemes[]" "known to those skilled in that art." EX1005, 17:7-14. However, merely encrypting information does not disclose how (or if) any device was authenticated such that it could decrypt information. Malek Dec., ¶¶ 53-54.

While Russ discloses utilizing DTCP's ***encryption*** scheme, it never discloses using it for any ***authentication***. Petitioner argues that Russ discloses authentication using an AKE key exchange between DSCT 110 and client-receiver 122, requiring "DTLA licensed certificates." Pet., 45. Petitioner's expert opines that DTLA certificates are "issued by a trusted authority" which establishes a "root of trust." While neither Petitioner nor its expert offer any explanation on this process,[1] the key exchange would provide the client-receiver 122 information, a "key," that could be used to decrypt communication. Malek Dec., ¶ 54. However, Russ does not disclose any AKE key exchange or any DTLA licensed certificates; instead, Russ discloses exchanging trusted keys without the need for DTLA certificates. *Id.*

Russ describes that a serial number and keys are assigned to a client-receiver and included in the client-receiver during the manufacturing process. Malek Dec., ¶

[1] Instead, it appears Petitioner ran a search to find the term "authenticate" near "DTCP," and came back with two non-peer reviewed patent publications.

54; EX1005, 26:29-48. The manufacturer provides the serial number and a key to the operator of Russ's DBDS (the subscriber network), which is the headend 102. Malek Dec., ¶ 54; *see also* Wasilewski Dec., ¶ 123 (acknowledging that headend 102 is the "operator of the DBDS 100"). When the device comes online, the DSCT 110 forwards the serial number of the device to the headend 102's CAA (content access authority). Malek Dec., ¶ 54; EX1005, 26:29-48. The headend then confirms whether it has received the serial number and keys from the manufacturer. Malek Dec., ¶ 54; EX1005, 26:29-48. If so, the CAA of the headend "sends the client-receiver 122 via, the DSCT, an EMM that includes the public key of the DSCT 110," and "the client-receiver 122 accepts the public key of the DSCT 110 as a trusted key." EX1005, 26:29-48. Russ thus describes a process of exchanging keys that does not involve AKE key exchange or certificates of the DTLA. Thus, Petitioner's alleged "AKE exchange" and "DTLA certificates" are not disclosed by Russ. As such, Petitioner fails to demonstrate that Russ discloses a second root of trust and ground 1 fails.

D. The Petition Fails to Demonstrate that Russ Discloses "a Second Root of Trust Which is Independent of and Different Than the First Root of Trust."

Even assuming Russ did teach an AKE exchange using DLTA certificates (it does not), it nevertheless fails to disclose "a second root of trust which is ***independent*** of and different than the first root of trust," as required by all challenged

claims. The claims require not only that the first root of trust is "different," but also a separate requirement that it is "independent." And as highlighted in prosecution, a root of trust is not "independent" just because it is different. *See, e.g.*, EX1002, 477-488 (a "child client public key" may have been different, but was not independent). Yet, that is precisely what Petitioner argues here. Petitioner and its expert fail to explain how Russ's purported second root of trust is ***independent*** from the purported first root of trust. Instead, they lump the separate requirements together and conclude that the two purported roots of trust are independent simply because they are different. Pet., 46 (Petitioner summarily concludes that "[c]ommunications between headend 102 and DSCT 110 do not use DTCP authentication procedures or certificates and are therefore independent and based on a different root of trust from that between DSCT 110 and client-receiver 122."). For this reason alone, the Petition must fail.

Moreover, any second root of trust in Russ is not independent of the alleged first root of trust. Petitioner contends the "first root of trust" is "serial numbers and keys" of the DSCT 100 that the network operator, at headend 102, uses to authenticate and establish communications with the DSCT. Pet., 44-45. Likewise, the alleged "second root of trust" is an exchange using information in client-receiver 112. *Id.*, 45.

With Petitioner's theory in mind, it is a stated purpose of Russ that the two purported roots of trust are ***not*** independent. Russ explains that the operator of a subscriber network system desires control over communications between the DSCT and subscriber devices, including to "control the type of devices that receive information from the DSCT or the type of content that the device receives." EX1005, 2:5-3:10. The operator thus "establish[es] secure communication with the client-devices and control[s] the content that is provided to the client-devices." *Id.* And the operator does this using the headend 102 and its system controller 232. *Id.*, 10:25-29 ("control system 232 … allows the DBDS system operator to control and monitor the functions and performance of the DBDS 100."). As such, the headend 102 controls any authentication of a client-receiver, controls what content it can receive, and can, at any time, remove a client-receiver as an authorized device. *See infra* Section III.B; Malek Dec., ¶¶ 58-59.

For the headend 102 to perform its job of controlling authentication and access to a client-receiver, it does so via the DSCT. That is, Russ's headend 102 establishes communications with the DSCT 110 (using the alleged first root of trust) and then the headend 102 controls the client-receivers via communications through the DSCT 110. Indeed, as Petitioner's expert concedes, the DSCT grants and deletes entitlements to service instances under the control of headend 102. Wasilewski Dec., ¶ 83.

Under Petitioner's theory, the purported second root of trust is initiated through "DTCP protocols" which are initiated after it is determined to use the DTCP encryption scheme for communications between DSCT 110 and client-receiver 122. Pet., 46. However, even the dynamic encryption is controlled by the headend 102, as Petitioner and its expert concede. Pet., 43-44 ("headend 102 … dictat[es] the encryption scheme for communications with client-receiver 122"); *see also* EX 1005, 25:17-22 ("headend 102 determines the encryption scheme used to communicate information between the DSCT 110 and the client-receiver 122"); *id.*, 14:50-55 (encryption scheme determined by tables sent from the headend 102 to DSCT 110). For the DSCT 110 to "determine" the encryption scheme, it requires instructions from the headend 102, and those communications are only provided after—and because of—establishing the alleged first root of trust between the headend 102 and DSCT 110. *See, e.g.*, EX1005, 7:56-8:3. Thus, without the alleged first root of trust, the alleged second root of trust cannot be established. In other words, any root of trust between the DSCT 110 is intrinsically tied to and predicated on a root of trust between the headend 102 and DSCT 110. The purported second root of trust therefore, while perhaps different, is far from ***independent*** from the first root of trust, as required by the challenged claims.

That the purported first and second roots of trust are not independent is highlighted by Petitioner's disparate theories with respect to the first and second

roots of trust. For the authentication of the DSCT 110 using the first root of trust requirement, Petitioner asserts that Russ discloses that "when DSCTs 110 connect to the DBDS, headend 102 authenticates a DSCT 110 by verifying that DSCT 100's unique serial number is in a database of serial numbers and corresponding keys that have been certified by the manufacturer." Pet., 44. With respect to the client-receiver, Russ has this same disclosure. EX1005, 26:29-48 (the client-receiver includes a serial number, which is stored in a database of the DBDS; when the client-receiver is brought onto the network, its information is forwarded to the headend 102 which registers the device and sends the client-receiver a trusted key "via the DSCT.").

According to Petitioner's theory for the first authentication, the client-receiver would thus be "authenticated" prior to any DTCP encryption or dynamic encryption determination. Tellingly, Petitioner and its expert ignored this disclosure of Russ for the second authentication requirement, because it highlights that it is the ***headend*** 102 performing any authenticating, and further that the alleged second root of trust cannot be established without the alleged first root of trust—the roots of trust are not independent, they are "chained," much like the art distinguished in prosecution. *See* EX1002, 477. This is apparently why Petitioner and its expert attempt to rely on a different purported authentication technique that is not disclosed in Russ. But even so, the theory fails for the same reason: As Russ's headend 102 controls the entire

DBDS network, any second root of trust between the DSCT 110 and client-receiver 122 cannot be established without the alleged first root of trust. Any purported second root of trust in Russ cannot be ***independent*** of the alleged first root of trust. The Petition fails.

In short, Russ fails to disclose a second root of trust that is independent from the first root of trust, as Russ teaches a different system aimed at serving a different purpose. As noted previously, Russ teaches a single "subscriber network" that is under the control of a single system operator. Malek Dec., ¶ 44 (discussing Russ). The '236 patent, on the other hand, teaches how to bridge together different networks under different control. *See, e.g.*, EX1001, Abstract. Indeed, as discussed above, this was a distinguishing feature in prosecution. 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 <u>independent</u> 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.

Russ teaches systems similar to those distinguished during prosecution. Russ fails for at least the same reasons as discussed there (i.e., there is independence between the first and second roots of trust). There is no reasonable likelihood of success on any challenged claim and the Petition fails.

E. Grounds 2-4 Cannot Demonstrate any Reasonable Likelihood of Success.

Petitioner's anticipation arguments for ground 1 fail for at least the two reasons discussed above. And the remaining grounds fail for the same reasons. While Petitioner alleges that Russ renders obvious the challenged claims for ground 2, it makes no effort to cure Russ's deficiencies discussed above with respect to ground 1. Instead, Petitioner vaguely argues that it would have been obvious to combine any of the discrete embodiments of Russ in any manner. Petitioner thus is only relying on the disclosures of Russ. And as discussed above, those disclosures are insufficient. While Petitioner adds additional references for grounds 3 and 4 for the dependent claims, the references do not cure Russ's deficiencies with respect to the independent claims, and Petitioner makes no assertion to the contrary. As such, there is no likelihood of success for any ground.

IV. The Board Should Deny Institution for Violating the "Particularity" Requirement.

The basis of an IPR petition must be identified "with particularity." *Adaptics Ltd. v. Perfect Co.*, IPR2018-01596, Paper 20, at 15 (P.T.A.B. Mar. 6, 2019)

(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). "The statutory requirement for particularity in a petition for IPR takes on heightened importance when considered in conjunction with *SAS*'s 'all-or-nothing' approach" of institution: because institution requires one binary choice for all grounds, every ground must meet the particularity requirement. *Adaptics*, Paper 20, at 17. When the Petition fails the particularity requirement for any ground, the Board may deny institution. *Id.*

Petitioner's "catch-all" obviousness contention of ground 2 fails to satisfy the particularity requirement. *See* Pet., 62. In ground 1, Petitioner contends that Russ anticipates each challenged independent claim. *Id.*, 22. In ground 2, Petitioner backtracks, arguing that "[t]o the extent PO argues that various relied-on features of Russ are from distinct and unrelated embodiments," it will later rely on any combination of the vague "various relied-on features." *Id.*, 62. However, Petitioner 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." *Id.* Petitioner's hedge, which explicitly seeks to wait and see what "PO argues" is impermissible, as Petitioner fails to satisfy its "burden from the onset" to particularly disclose its theories. *See*

Harmonic, 815 F.3d at 1363. The Board should not allow Petitioner's "wait and see" approach, which attempts to disclose obviousness theories for the first time in Reply.

V. CONCLUSION

As the actual disclosure of Russ highlights its deficiencies, Petitioner is forced to invent new disclosure that is not present in Russ. But doing this only exacerbates the failures of the Petition. The Board should deny institution of *inter partes* review.

Dated: September 18, 2024

/Jerry D. Tice II/
Jerry D. Tice II
Reg. No. 73,582
Bunsow De Mory LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-351-7248
Facsimile: 415-426-4744
jtice@bdiplaw.com

Lead Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

1. This Patent Owner's Preliminary Response complies with the type-volume limitation of 14,000 words, comprising 5,426 words, excluding the parts exempted by 37 C.F.R. § 42.24(a)(1).

2. This Patent Owner's Preliminary Response complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14 point Times New Roman.

Dated: September 18, 2024

/Jerry D. Tice II/
Jerry D. Tice II, Reg. No. 73,582

CERTIFICATE OF SERVICE

Petitioner has consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that on September 18, 2024, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

Wolf, Greenfield & Sacks, P.C.
Scott A. McKeown – SMcKeown-PTAB@WolfGreenfield.com
Libbie A. DiMarco - Elizabeth.DiMarco@WolfGreenfield.com
Victor Cheung - VCheung-PTAB@WolfGreenfield.com

Dated: September 18, 2024

/Jerry D. Tice II/
Jerry D. Tice II, Reg. No. 73,582