UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

HISENSE USA CORPORATION; and
HISENSE ELECTRONICA MEXICO S.A. de C.V.
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner

Case IPR2025-00881
U.S. Patent 8,291,236

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. THE '236 PATENT 2

III. THE BOARD NEED NOT REACH ANY CLAIM CONSTRUCTION ISSUES TO DENY THE PETITION 4

IV. PETITIONER'S CHALLENGES FAIL ON THE MERITS 5

A. Ground 1 Based on Russ Fail 5

1. Russ's Headend Oversees All Device Authorization 5

2. Russ fails to disclose or suggest the features of independent claims 48, 82, 116, and 140 9

B. Ground 2 is conclusory and fails 13

V. CONCLUSION 13

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Digital Keystone (available at https://en.wikipedia.org/wiki/Digital_Keystone)
2002	VideoLabs Licensees (available at https://www.videolabsinc.com/licensees)
2003	Hisense (available at https://en.wikipedia.org/wiki/Hisense)
2004	Email thread between VideoLabs and Hisense (Dec. 27, 2022 to June 7, 2023)
2005	Letter from Goldman to Gold, Hisense and VideoLabs' Intellectual Property (Dec. 27, 2022)
2006	VideoLabs – Hisense Licensing Discussion, Claim Charts for US-8291236 & US-8667304 (Jun. 7, 2023)
2007	Complaint, *VideoLabs v. Hisense Co. Ltd.*, Civ. No. 2:24-cv-904 (E.D. Tex. Nov. 6, 2024)
2008	LinkedIn post from VideoLabs concerning Roku (available at https://www.linkedin.com/posts/videolabs-inc_videolabs-the-leading-patent-licensing-activity-7287514328054824960-AUG0/)
2009	LinkedIn post from VideoLabs concerning ASUS (available at https://www.linkedin.com/posts/videolabs-inc_videolabs-is-pleased-to-announce-asus-as-activity-7353091447769763841-WqLK/)
2010	Special Master's Report and Recommendation Regarding Claim Construction, *VideoLabs, Inc. v. Asus Computer Int'l*, Case No. 6:22-cv-00720 (W.D. Tex. Mar. 21, 2025)
2011	Claim Construction Order, *VideoLabs, Inc. v. HP Inc.*, Case No. 6:23-cv-00641 (W.D. Tex. Aug. 26, 2024)

Pursuant to 35 U.S.C. § 313, VideoLabs, Inc. ("VideoLabs" or "Patent Owner") files this patent owner's preliminary response, setting forth reasons why the Petition for *inter partes* review ("IPR") of claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 of U.S. Patent 8,291,236 (the "'236 patent"), as requested by Hisense USA Corporation and Hisense Electronica Mexico S.A. de C.V. ("Hisense" or "Petitioner"), should be denied.

I. INTRODUCTION

Each challenged claim of the '236 patent recites a conditional access server "configured to substitute" a first security domain with a second security domain. *See* independent claim 140; *see also* independent claims 48, 82, and 116. Russ, relied on by Petitioner as an anticipatory reference, fails to show any substitution of a first security domain with a second security domain because, in Russ, a single entity (headend 102, an "operator") authenticates the entire network including DSCT 110 (which Petitioner alleges is a conditional access server) and client-receiver 122 of the DSCT 110. Accordingly, for this simple reason and the other reasons set forth below, Russ fails to disclose or suggest every claimed feature of the challenged claims, and Petitioner's challenge fails.

A separate deficiency of the Petition is its failure to meet the particularity requirement for ground 2. There, Petitioner argues that Russ renders obvious the challenged independent claims, but 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. The Petition fails to identify any embodiment of Russ or any feature(s) of other embodiments that it seeks to combine. 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 should be rejected for failing to state Petitioner's proposed obviousness challenge with particularity.

Petitioner suggests that institution is required here because "the Board previously instituted *inter partes* review of the '236 [patent] based on an identical petition. *Roku, Inc. v. VideoLabs, Inc*., IPR2024-01024, paper 12 (PTAB Dec. 4, 2024)." Pet., 1. However, the technical arguments presented in this POPR were not before the panel at institution stage in IPR2024-01024, and these technical arguments warrant denial here.

For the reasons introduced above and presented more fully below, the Petition should be denied, and no IPR should be instituted.

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. '236 patent, cover page. It is related to conditional access (CA), "a technique for limiting the access of content (e.g., audiovisual works such as movies) to authorized users." *Id*., 1:13-15.

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 (emphasis added). 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*., 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*. Indeed, as explained in the '236 patent, "entities not known in the primary security domain can be provisioned through the use of the secondary CA server, which has an identity known in the primary security domain and knows the entities in the secondary security domain." '236 patent, 8:12-16. This allows for "two security systems having two independent authentication processes." EX1002, 479.

III. THE BOARD NEED NOT REACH ANY CLAIM CONSTRUCTION ISSUES TO DENY THE PETITION

Petitioner contends that a dispute exists concerning a term appearing in claim elements 48[a], 82[a.ii], 116[a], and 140[a.ii], but asserts "construction of this term is not necessary at this time." Pet., 17. Without waiving its right to submit constructions in a Patent Owner Response, Patent Owner submits that the Board need not engage in any pre-institution claim construction because the Petition fails to establish invalidity of any challenged claim under the plain and ordinary meaning of each term.[1] For the substantive reasons presented in Section IV below, Petitioner's grounds include fundamental flaws and fail to establish the disclosure of every claimed element in each independent claim. These findings do

[1] Claim construction has been considered in two district court litigations (*see* Ex. 2010 and Ex. 2011), but these orders, and the constructions reached therein, do not bear on the technical merits arguments presented below.

not require the Board to conduct any construction of the above-identified claim elements.

IV. PETITIONER'S CHALLENGES FAIL ON THE MERITS

Petitioner raises only two grounds in its Petition. Ground 1 contends that independent claims 48, 82, 116, and 140 (and certain identified dependent claims) are anticipated by Russ[2]. Ground 2 presents an undeveloped obviousness theory based on Russ alone.

A. Ground 1 Based on Russ Fail

1. Russ's Headend Oversees All Device Authorization

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" ('236 patent, 8:12-21), Russ is like the art discussed during prosecution and is directed to a single "subscriber network" system wherein content access and authorization is controlled by a single administrative component, Russ's "headend 102." Russ, claim 1. Russ describes a conventional broadband system, such as a cable or satellite television system. Russ, 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

[2] EX1005, U.S. Patent 6,748,080 ("Russ").

terminal (DSCT) connected to a subscriber's devices (TV and laptop) with a wired and wireless connection. *Id.*, Fig. 1. As explained in more detail below, the headend 102 provides content to subscriber devices within the subscriber network. *See*, *e.g.*, Russ, 1:15-19. The headend acts as an operator for the system—managing encryption of communications between devices in the network and also managing which devices in the network are authenticated for receiving content. Russ, 25:17-22.

Like conventional systems, Russ's system included, at "a subscriber location, a digital subscriber communications terminal (DSCT)," such as a set-top box. *See* Russ, 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 introduces security and control concerns, and 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. Russ discloses that "[s]ystem tables are prepared by the control system 232 [of headend 102] and transmitted to the DSCT 110." Russ, 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.

Russ also 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." Russ, 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."). Because 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.

Serving as the operator, the 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.

According to Russ, 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. Thus, while a DSCT in a subscriber's home passes content to a client-receiver, the network operator—via the headend—controls what content can be provided to which device and how that content is delivered. *See id.*, 19:16-27.

2. Russ fails to disclose or suggest the features of independent claims 48, 82, 116, and 140

As noted above, each challenged independent claim of the ’236 patent recites a conditional access server “configured to substitute” a first security domain with a second security domain. *See* independent claim 140; *see also* independent claims 48, 82, and 116. However, Russ fails to disclose or otherwise suggest any substitution of a first security domain with a second security domain. This is because, as explained above, a single entity (headend 102, an “operator”) authenticates the entire network including DSCT 110 (which Petitioner alleges is a conditional access server) and client-receiver 122 of the DSCT 110.

Russ’s failure to disclose or suggest a substitution of security domains, and other claimed aspects, is evident from Russ’s registration procedures for the initial connection of the DSCT 110 and client-receiver 122. Russ discloses registering the DSCT 110 as follows (Russ, 7:56-66):

> Before the DSCT 110 receives and accesses service instances from the headend 102, the DSCT 110 is registered with the headend 102 and entitled to the service instances. When the DSCT 110 is connected to the DBDS 100, it sends a message, which includes the serial number of the DSCT 110, to the headend 102. The operator of the DBDS 100 compares the serial number of the DSCT 110 against its database and registers the DSCT 110 if the

> database includes the serial number of the DSCT 110. Generally, the operator of the DBDS 100 replaces one of the trusted public keys of the DSCT 110 with its own trusted public key.

Here, the registration process authenticates DSCT 110 after checking a database and provides its public key to DSCT 110.

Russ's registration process for client-receiver 122 confirms that the DSCT (or any other component of the DBDS) does not perform any substitution of the primary security domain. As Russ explains with regard to FIG. 9 (Russ, 26:29-48) (emphasis added):

> When the client-receiver 122 is first brought into the local network of the DSCT 110, ***it negotiates a communication protocol with the DSCT 110*** and sends the DSCT 110 its public key. ***The DSCT 110 sends a secure message to the CAA 234 informing the CAA 234 that the client-receiver 122 is attempting to register***. The CAA 234 determines whether or not the client-receiver 122 is included in its database 240, and if it is, the CAA 234 initiates registration, which can include exchanging one of the trusted public keys of the client-receiver 122 with the public key of the CAA 234. The CAA 234 sends the client-receiver 122 via, the DSCT, an EMM that includes the public key of the DSCT 110, which is then stored in the

> secure element 908. The client-receiver 122 accepts the public key of the DSCT 110 as a trusted key.

Importantly, even after the client-receiver 122 has negotiated "a communication protocol" with the DSCT 110, registration is incomplete because the client has not been authenticated (using CAA 234 in headend 102 (*see* Fig. 2 of Russ)). Instead, the DSCT must send a "secure message" to headend 102, allowing the headend to check its database and initiate registration.

Petitioner's attempt to make the square peg of Russ fit into the round hole of the claim fails at multiple points. Each claim recites that "the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process." But as noted above, even after a client-receiver 122 has negotiated a communication protocol with the DSCT 110, the DCST must send a "secure message" to the headend 102. Because the DCST 110 cannot send a "secure message" to headend 102 until the DCST 110 itself is registered via the "first authentication process," the "second authentication process" is not "independent" of the "first authentication process." Rather, the "second authentication process" is dependent upon "first authentication process."

Petitioner's reliance on DTCP communication protocols and certificates for the alleged independence of the second authentication process and security domain

substitution (*see* Pet., 44-45) also fails. After a communication protocol is used to allow communication between the DCTP and the client-receiver, Russ explicitly requires the DSCT to send a secure message to the headend 102 before registration of the client-receiver 122. Thus, even where the DTCP protocol is used to establish communication between the DSCT 110 and client-receiver 122, no substitution of the first security domain with the second security domain occurs. Petitioner's DCTP theory fails to establish that "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."

Indeed, instead of showing any substitution of security domains, Petitioner's theories describe how communication occurs after the headend 102 has registered the devices to accept them into the single domain of Russ. Petitioner's reliance on Fig. 6 of Russ (Pet., 49) does not show any "substitution" of security domains but instead shows how messages flow within Russ after the devices have been registered. In other words, Fig. 6 of Russ shows message encryption, not the claimed device authentication and a substitution of one security domain with another.

Accordingly, Ground 1 fails because it has no reasonable likelihood of success.

B. Ground 2 is conclusory and fails

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., 68-69. 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.

V. CONCLUSION

Because Grounds 1-2 fail to show a reasonable likelihood of success, the Board should reject the Petition and deny institution of *inter partes* review.

Dated: September 24, 2025

/*Wayne M. Helge/*
Wayne M. Helge, Reg. No. 56,905
James T. Wilson, Reg. No. 41,439
BUNSOW DE MORY LLP
277 S. Washington St., Suite 210 #1088
Alexandria, VA 22314
T: (571) 208-0186
Email: whelge@bdiplaw.com
Email: jwilson@bdiplaw.com

Counsel for Patent Owner

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

The undersigned certifies that the foregoing PATENT OWNER'S PRELIMINARY RESPONSE complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the brief contains 2,859 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

Dated: September 24, 2025

/*Wayne M. Helge*/
Wayne M. Helge, Reg. No. 56,905

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 the date set forth below, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

Bas de Blank –M2BPTABDocket@orrick.com
Xiang Wang – XW0PTABDocket@orrick.com
Richard Martinelli – RFMPTABDocket@orrick.com
Thomas A. James – PTABDocketT6J1@orrick.com

Dated: September 24, 2025

/Wayne M. Helge/
Wayne M. Helge, Reg. No. 56,905