UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner.

Case No. IPR2024-01023
Patent No. 8,291,236

PETITIONER'S REPLY
TO PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

TABLE OF CONTENTS i
I. ’236 Patent and PO Representations 2
II. RUSS 4
CERTIFICATE OF SERVICE UNDER 37 C.F.R. §42.6(e)(4) 7

Patent Owner ("PO") does not dispute that Russ (EX1005) discloses different authentication processes using different first and second roots of trust. Russ's roots of trust are also independent of each other, for example, because each grants permissions to and from different entities, each uses different criteria, and the corresponding authentication decisions are not dependent on the output of the other. The '236 patent (EX1001; "'236") claims require nothing more.

Instead, PO argues that "independent" as used to modify the first and second roots of trust must be construed as ***independently controlled.*** But this is inconsistent with the claims, their supporting specification, and PO's infringement positions represented to the Federal Court (EX1008). 35 U.S.C. § 301(a)(2).

First, PO construes "independent" in a vacuum, divorced from its claims. For example, independent claim 66 of the '236 is directed to program instructions executed by the system to operate the first and second security domains. Far from excluding coordinated operations between first and second roots of trust, claim 66 explicitly recites system stored program instructions to manage operations of both.

The embodiments in the patent likewise show coordination among servers and between multiple security domains. Consistently, the specification examples identify a "***primary***" server (first conditional access server) communicating with a "***secondary***" server (second conditional access server) to "***control*** premium content distribution to ***external devices secured by a secondary*** security system." '236, 2:56-

59. Even assuming *arguendo* that PO identifies an embodiment where control of the primary server were somehow isolated and disconnected form the secondary such that there is no coordination, the claims cannot be so limited. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1369-70 (Fed. Cir. 2004) (cautioning against reading limitations into a claim, absent clear disclaimer). The specification explains that the claimed system distributes content that is authorized through a client server relationship between two independent and different roots of trust—just like Russ.

I. '236 Patent and PO Representations

PO insists that the prior art authentication processes' roots of trust are not "independent" of one another because the second authentication process is coordinated with the first authentication process. For example, PO argues that Russ's second authentication process using a second root of trust (in a second domain between a DSCT 110 and client-receiver 122) can only occur with instructions from a headend 102 (that is in a first domain) "after—and because of—establishing the alleged first root of trust between the headend 102 and DSCT 110." POPR, 19. But the manner of initial system set-up is not recited in the claims, nor does such a set-up cause a second root of trust to somehow collapse into the first such that there is now only a single trust determination.

PO next argues its narrowing construction is supported by the prosecution history, but this is false. PO insists that "as highlighted in prosecution, a root of trust

is not 'independent' just because it is different." POPR, 17 (citing EX1002, 477-488). Setting aside the strawman that Petitioner conflated the two terms, the prosecution arguments distinguish only a pure "proxy" authentication process. *See* POPR, 8-9 (no independent roots of trust where "a parent client could 'act as authentication proxy' for child clients in the same DRM system"), 13 ("a mere proxy fails to teach or suggest the challenged claims," referencing EX1002, 478). The prosecution history does not even address—let alone clearly disclaim—*any* relationship between the authentication processes or, more narrowly, control of a primary server by coordinating instructions or parameters at set-up for use in a secondary server's independent and different authentication of a client device.

The specification of the '236 is clear that a controlling relationship may exist between primary and secondary servers, and all that is required is 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. For example, the '236 explains that "the secondary CA server follows rules (e.g., CA messages) of the primary CA server to manage a secondary subscriber management system," including the independent root of trust authenticating secondary clients. '236, 8:16-38. *See also*, *e.g.*, '236, 2:56-59, 3:29-30, 3:33-36, 3:52-55, 4:1-3, 7:23-31, 8:50-53, 16:32-38, 16:39-45 (illustrating primary server control over the secondary server's content distribution).

In the District Court, PO accuses Roku products of doing exactly what it attempts to distinguish here. For example, PO accuses systems that include "PlayReady"-based components for authentications in a primary security system and "HDCP"-based components for authentications in a secondary security system. EX1008, 18-22 (discussing claim "130[c]" and "130[d]"). Under PO's infringement theory, the primary security system sets downstream restrictions on the secondary security system, including "HDCP enforcement requirements" that indicate "whether HDCP is required." EX1008, 9-10 (discussing claim "130[a]"), 15-17 (discussing claim "130[b]"). Yet, while the PlayReady primary system therefore "controls" the use of HDCP in the secondary system based on the POPR argument, PO still accuses the systems of infringement.

Therefore, independent authentication processes and roots of trust as claimed do not exclude systems where an independent process of one trust domain has some level of coordination with a second trust domain that is independent of the first. Indeed, absent some level of coordination at least at system set-up, there is no way to ensure "different authentication schemes" as claimed. "Independent," as claimed, identifies how the first and second roots of trust are used to arrive at their first and second authentication determinations, without relying on the output of the other.

II. RUSS

Russ describes a system including, *e.g.*, a headend 102, DSCT 110, and client-

receiver 122. EX1005, Fig. 1. Russ is no different from systems described in the ’236 and discloses the claimed independent authentication and roots of trust.

For example, DSCT 110 authenticates client-receiver 122 by “using [DTCP] protocols, which includes an authentication process” “based on an Authentication and Key Exchange (AKE) using DTLA licensed certificates, which is independent and different than the first authentication process’s and the first of trust’s use of serial numbers and keys between the headend 102 and DSCT 110” Petition, 40-41 (discussing claim “130[c.ii],” citing Russ, 16:64-17:14, and DTCP protocols in EX1010 and EX1011); *see also* Petition, 39-40 (discussing claim “130[c.i],” citing Russ, 7:21-39, 7:56-66; *also* 7:40-55, 8:4-11, 10:39-47).

Even if DTCP protocols would only be used by DSCT 110 (in a second security domain) because of some initial instruction issued by headend 102 (in a first security domain), as PO appears to argue (based on an incorrect interpretation of Russ nonetheless), that simple coordination is still in accordance with the patent specification and history, as discussed above, because the actual authentication processes are carried out independently.

Dated: October 11, 2024

Respectfully submitted,

By: /Scott A. McKeown/
Scott A. McKeown, Reg. No. 42,866
WOLF, GREENFIELD & SACKS, P.C.

Counsel for Petitioner
Roku, Inc.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. §42.6(e)(4)

I certify that on October 11, 2024, I will cause a copy of the foregoing document, including any exhibits or appendices filed therewith, to be served via electronic mail, as previously consented to by Patent Owner, upon the following:

Jerry D. Tice II	jtice@bdiplaw.com
Aaron R. Hand	ahand@bdiplaw.com
	VideoLabs_Roku@bdiplaw.com

Date: October 11, 2024

/Dara Del Rosario/
Dara Del Rosario
Paralegal
WOLF, GREENFIELD & SACKS, P.C.