

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner.

Case No. IPR2024-01026
Patent No. 8,667,304

PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 *et seq.*

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
TABLE OF AUTHORITIES	iii
TABLE OF EXHIBITS	iv
I. INTRODUCTION	1
II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	7
A. Real Party-In-Interest	7
B. Related Matters.....	7
C. Lead and Back-up Counsel, and Service Information	8
III. REQUIREMENTS FOR IPR	8
A. Grounds for Standing (37 C.F.R. §42.104(a))	8
B. Identification of Challenge (37 C.F.R. §42.104(b)).....	8
1. Specific Art on Which the Challenge is Based.....	8
2. Statutory Grounds on Which the Challenge is Based.....	9
IV. BACKGROUND	9
A. '304 Patent.....	9
B. Prosecution History of the '304	12
C. Prosecution History of the '236	13
V. LEVEL OF ORDINARY SKILL IN THE ART.....	14
VI. CLAIM INTERPRETATION	15
A. “content that is in an access controlled format specified by the second conditional access server”	15
VII. GROUNDS OF UNPATENTABILITY.....	16
A. Ground 1: Claims 5-6, 8, 16-17, and 19 are Anticipated by Russ	17
1. Overview: Russ	17
2. Claim Charts (5-6, 8)	20
3. Claim Charts (16-17, 19)	44
B. Ground 2: Claims 5-6, 8, 16-17, and 19 are Obvious Over Russ	48

C.	Ground 3: Claims 7 and 18 are Obvious Over Russ in view of Robert	49
1.	Overview: Robert	49
2.	Motivation: Russ in view of Robert.....	51
3.	Claim Charts (7, 18).....	54
VIII.	NO BASIS FOR DISCRETIONARY DENIAL	56
A.	<i>Fintiv</i>	56
B.	<i>Advanced Bionics</i>	57
IX.	CONCLUSION.....	58
	CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (e)(4)	59
	CERTIFICATE OF WORD COUNT	60

TABLE OF AUTHORITIES

CASES

<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	56
<i>Bowtech, Inc. v. MCP IP, LLC</i> , IPR2019-00379, Paper 14 (PTAB July 3, 2019)	58
<i>In re Arkley</i> , 455 F.2d 586 (C.C.P.A. 1972)	20
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	53
<i>Net MoneyIN, Inc. v VeriSign, Inc.</i> , 545 F.3d 1359 (Fed. Cir. 2008).....	20
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017).....	15
<i>Nokia of Am. Corp. v. TQ Delta, LLC</i> , IPR2022-00471, Paper 11 (PTAB Aug. 18, 2022)	56

TABLE OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 8,667,304 (“’304”)
1002	File History of U.S. Patent Application No. 13/612,663 (“’304FH”)
1003	Declaration of Anthony J. Wasilewski, Ph.D. (“Wasilewski”)
1004	CV of Anthony J. Wasilewski, Ph.D.
1005	U.S. Patent No. 6,748,080 (“Russ”)
1006	U.S. Patent No. 7,546,641 (“Robert”)
1007	RESERVED
1008	<i>VideoLabs, Inc. v. Roku, Inc.</i> , Case No. 1:23-cv-01136 (D. Del.), Dkt. No. 1, Complaint Exhibit 11 – U.S. Patent No. 8,291,236 (“’236 Patent”) (Oct. 11, 2023)
1009	<i>VideoLabs, Inc. v. Roku, Inc.</i> , Case No. 1:23-cv-01136 (D. Del.), Dkt. No. 1, Complaint Exhibit 12 – U.S. Patent No. 8,667,304 (“’304 Patent”) (Oct. 11, 2023)
1010	U.S. Patent Application Publication No. 2002/0025042
1011	U.S. Patent Application Publication No. 2005/0027984
1012	U.S. Patent Application Publication No. 2003/0078891
1013	U.S. Patent Application Publication No. 2004/0098583
1014	RESERVED
1015	File History of U.S. Patent Application No. 11/007,116 (“’236FH”)
1016	Federal Judicial Caseload Statistics (Dec. 31, 2023)
1017	RESERVED

I. INTRODUCTION

Petitioner Roku, Inc. (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 5-8 and 16-19 (“Claims”) of U.S. Patent No. 8,667,304 (EX1001; “’304”) assigned to VideoLabs, Inc. (“PO”) in accordance with §§311-319 and §42.100 et seq. There is a reasonable likelihood that at least one challenged claim is unpatentable as explained herein. Petitioner requests review of the Claims, and judgment finding them unpatentable under §§102-103.

Efforts to protect media content during and after transmission, like movies distributed via cable television, have led to the development of a variety of content protection schemes. ’304, 1:9-13; *see also* EX1006 (“Robert”), 1:21-25. Two well-known schemes implemented in content protection systems are conditional access (CA) and digital rights management (DRM). ’304, 1:15-2:55; Robert, 1:28-30.

In a CA system, content is scrambled or encrypted by a key known as a control word (CW), which is conveyed to user devices via entitlement control messages (ECMs) and itself encrypted by a service key. ’304, 1:23-35, 1:29-35, 1:36-38; Robert, 4:27-30, 4:49-51. The service key is conveyed separately via entitlement management messages (EMMs) and encrypted by a user key typically unique to each user device. ’304, 1:45-60; Robert, 4:51-59. Thus, CA systems protect content via several levels of encryption and CA messages.

In a DRM system, content is encrypted, and rights to the content are obtained separately, for example from a license issuer. '304, 2:34-43; Robert, 4:64-5:58. Typically a single key is provided to decrypt the content in a DRM system. Robert, 5:52-58.

The '304 is also directed to systems for limiting the access of audiovisual content. '304, 1:9-13. The '304 purports to “bridg[e] two security systems” including a primary security system “used to secure the distribution of premium content only to legitimate subscribers,” and a secondary security system “used to secure the distribution of premium content only to the legitimate devices of the subscriber.” '304, 2:59-3:3. Thus a system according to the '304 may include a primary server distributing content to a secondary server that re-distributes the content to secondary clients. '304, 2:64-4:5.

As shown in Fig. 2A below, for example, **secondary CA server 255** is in communication with both **primary CA server 253** (in primary security domain 251) and with **clients 271, 273, ..., 279** (in secondary security domain 261). '304, 7:8-43.¹ In the primary security domain, **secondary CA server 255** acts as a client and processes control information for the conditional access of content provided by **primary CA server 253**. '304, 7:33-39. In the secondary security domain,

¹ In this Petition, emphases and annotations are added unless noted otherwise.

secondary CA server 255 acts as a control information provider to conditionally allow secondary CA **clients** to access the content. '304, 7:37-43. In this way, “secondary CA clients in the secondary security domain may access the content secured in the secondary security domain under the control of the secondary CA server in accordance with security messages provided by the primary security domain to the secondary CA server.” '304, 7:26-31 (reference numerals omitted).

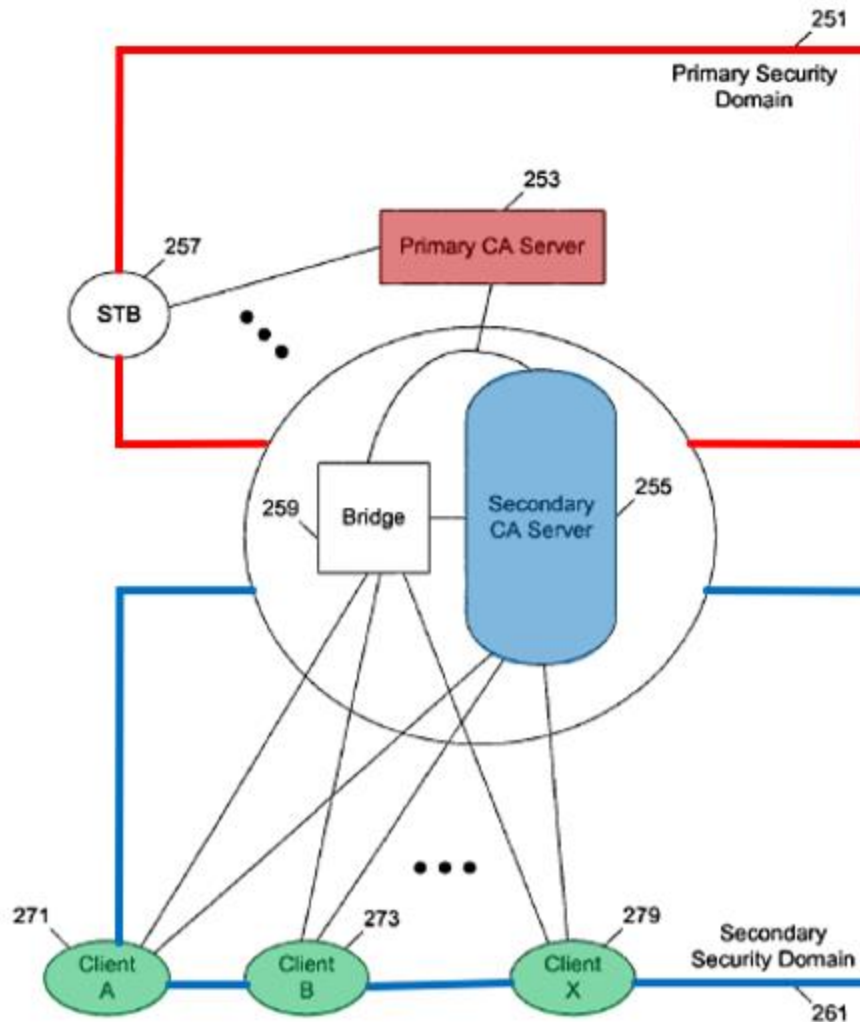
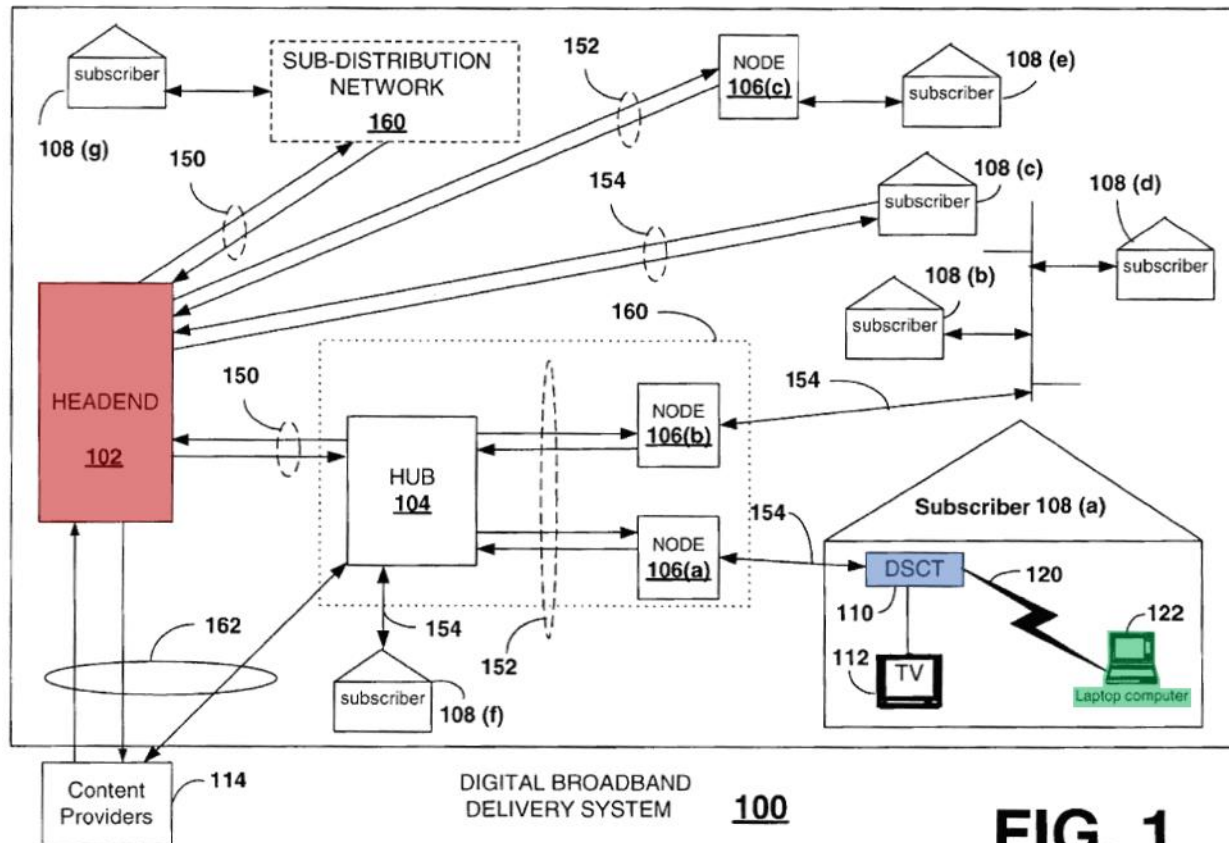


Fig. 2A

Stated more simply, the primary server provides content to an authorized secondary server, and the secondary server provides content to authorized clients. In different embodiments, both servers use CA techniques or DRM techniques, or one server may use CA techniques while the other uses DRM techniques, for example. '304, 2:64-3:18.

But the bridging of two security systems was well-known in the art. For example, Russ (EX1005) discloses a digital subscriber communications terminal (DSCT) that receives CA content and entitlements from a headend and that, furthermore, manages a local network of client-receivers and serves content and entitlements using encryption schemes specific to the identity of each client device—some such devices requiring DRM techniques like Digital Transmission Content Protection (DTCP) and Content Protection for Recordable Media (CPRM). Russ, 3:11-22, 7:56-8:22, 8:38-9:7, 10:48-65, 16:64-17:14, 18:29-51. *See* Fig. 1 (showing **headend 102** as a primary server serving **DSCT 110**, and **DSCT 110** as a secondary server serving **client-receiver 122**).



Russ's system therefore bridges security systems, like the '304. Russ therefore anticipates claims 5-8 and 16-19 of the '304. Additional features claimed in dependent claims, like the transmission of specific data including decrypted ECMs and control words, were also well known, as evidenced by Robert (EX1006) discussed below. The USPTO did not consider Russ, alone or in combination with Robert, during the '304's prosecution.

Accordingly, Petitioner respectfully requests that the Board institute trial and cancel the Claims.

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Party-In-Interest

Petitioner identifies Roku, Inc. as real party-in-interest. No other party had access to or control over the present Petition, and no other party funded or participated in preparation of the present Petition.

B. Related Matters

The '304 is currently asserted in the following district court proceedings:

Title	No.	Court	Filing Date
<i>VideoLabs, Inc. v. Roku, Inc.</i>	1:23-cv-01136	D. Del.	2023-10-11
<i>VideoLabs, Inc. v. HP Inc.</i>	6:23-cv-00641	W.D. Tex.	2023-08-31
<i>VideoLabs, Inc. v. ASUSTeK Computer Inc.</i>	6:22-cv-00720	W.D. Tex.	2022-06-30

Petitioner is also concurrently filing petitions for *inter partes* review with respect to U.S. Patent No. 8,291,236, to which the '304 claims to be a continuation, and recommends assigning all petitions to the same panel.

Title	Patent	IPR No.
<i>Roku Inc. v. VideoLabs, Inc.</i>	8,291,236	IPR2024-01023
		IPR2024-01024
		IPR2024-01025
<i>Roku Inc. v. VideoLabs, Inc.</i>	8,667,304	IPR2024-01026

C. Lead and Back-up Counsel, and Service Information

Lead Counsel	Scott A. McKeown, Reg. No. 42,866	
Backup Counsel	Libbie A. DiMarco (<i>pro hac vice</i> forthcoming) Victor Cheung, Reg. No. 66,229	
Service Information	E-Mail	SMcKeown-PTAB@WolfGreenfield.com Elizabeth.DiMarco@WolfGreenfield.com VCheung-PTAB@WolfGreenfield.com
	Post & Hand-Delivery	Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210-2206
	Telephone	(617) 646-8000
	Facsimile	(617) 646-8646

Petitioner consents to electronic service of documents to the email addresses of the counsel identified above.

III. REQUIREMENTS FOR IPR

A. Grounds for Standing (37 C.F.R. §42.104(a))

Petitioner certifies the '304 is available for IPR and Petitioner is not barred or estopped from requesting IPR on the following grounds.

B. Identification of Challenge (37 C.F.R. §42.104(b))

Petitioner requests IPR of the Claims and that the Board cancel the same as unpatentable.

1. Specific Art on Which the Challenge is Based

Petitioner relies upon the following prior art:

Name	Ex.	Patent / Publication	Filing Date	Publication Date	Prior Art Under at Least Pre-AIA §102
Russ	1005	6,748,080	2002-05-24	2004-06-08	(a)/(e)
Robert	1006	7,546,641	2004-02-13	2009-06-09	(e)

2. Statutory Grounds on Which the Challenge is Based

Petitioner respectfully requests cancellation of the Claims on the following grounds:

Ground	Basis	Claims	Reference(s)
1 / 2	§102 / §103	5-6, 8, 16-17, 19	Russ
3	§103	7, 18	Russ in view of Robert

IV. BACKGROUND

A. '304 Patent

The '304 discusses methods and apparatuses for bridging two security systems for content delivery in cable television systems, satellite television systems, and the like. '304, 1:9-13, 2:59-62. Such security systems are known and, for example, use “conditional access (CA)” or “digital rights management (DRM)” techniques. '304, 1:17-2:55.

As discussed in §I above, Fig. 2A below shows **secondary CA server 255** as a client of **primary CA server 253** (in primary security domain 251) and as a control information provider for **clients 271, 273, ..., 279** (in secondary security domain 261). '304, 7:8-43. Through the **secondary CA server 255's** bridging,

clients secured under control of the secondary CA server 255 may access secure content provided to the secondary CA server 255 by primary CA server 253.

'304, 7:26-31.

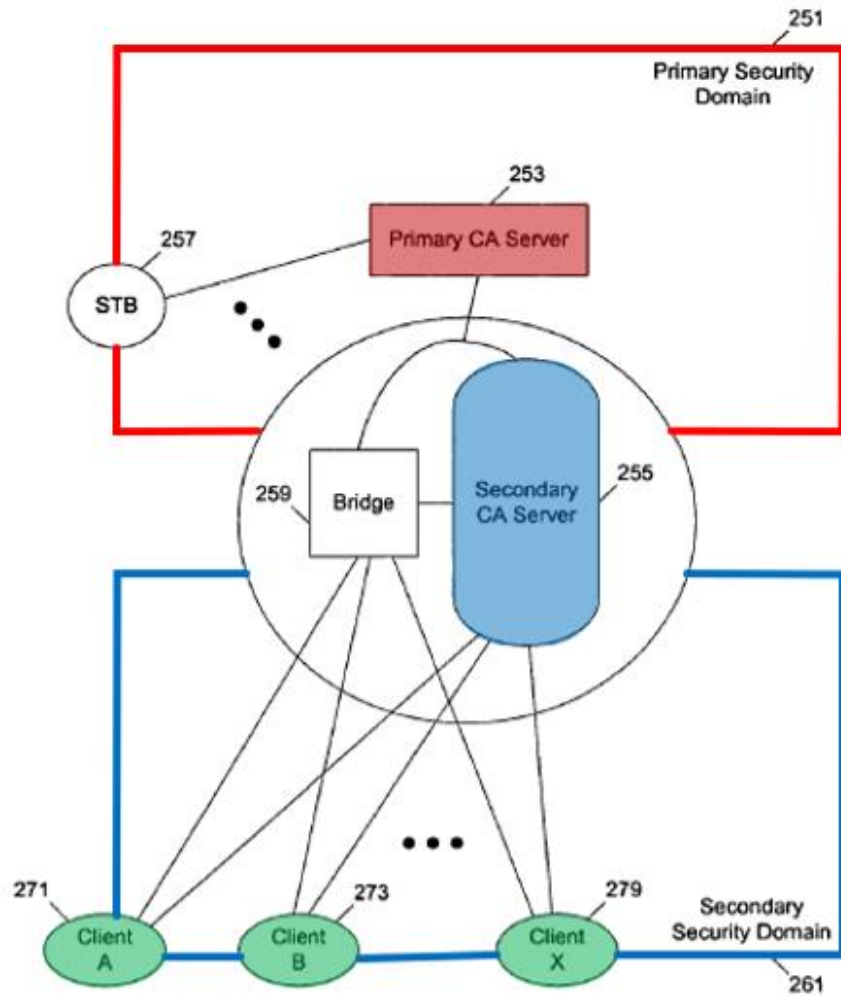


Fig. 2A

And, as discussed, while Fig. 2A shows two CA servers, different embodiments alternatively use DRM techniques or a mix of CA and DRM techniques. '304, 2:64-3:18. Accordingly, bridging in the '304 involves a primary

server providing content to an authorized second server, and the second server re-distributing the content to authorized clients.

The '304 describes several scenarios incorporating known content protection techniques into the bridging concept. For example, Fig. 11 below shows **bridge 603** and **secondary CA server 609**—which are shown separately but may be physically and functionally combined with each other and with **storage 605** (see '304, 17:16-41, 18:9-18)—receiving a broadcast feed 601 from a primary security system (not shown). '304, 17:52-61. Content 611, entitlement control message (ECM) 613, and entitlement management message (EMM) 615 are protected by a control word, service key, and user key, respectively. '304, 17:55-61. However, **renderer 607** wanting access to the content is provided with the control word 619 only protected by DRM after the **secondary CA server 609** itself decodes the ECM to obtain the control word—thus **renderer 607** with appropriate DRM rights will be able to decode the control word-scrambled content without the service key and user key. '304, 18:44-54.

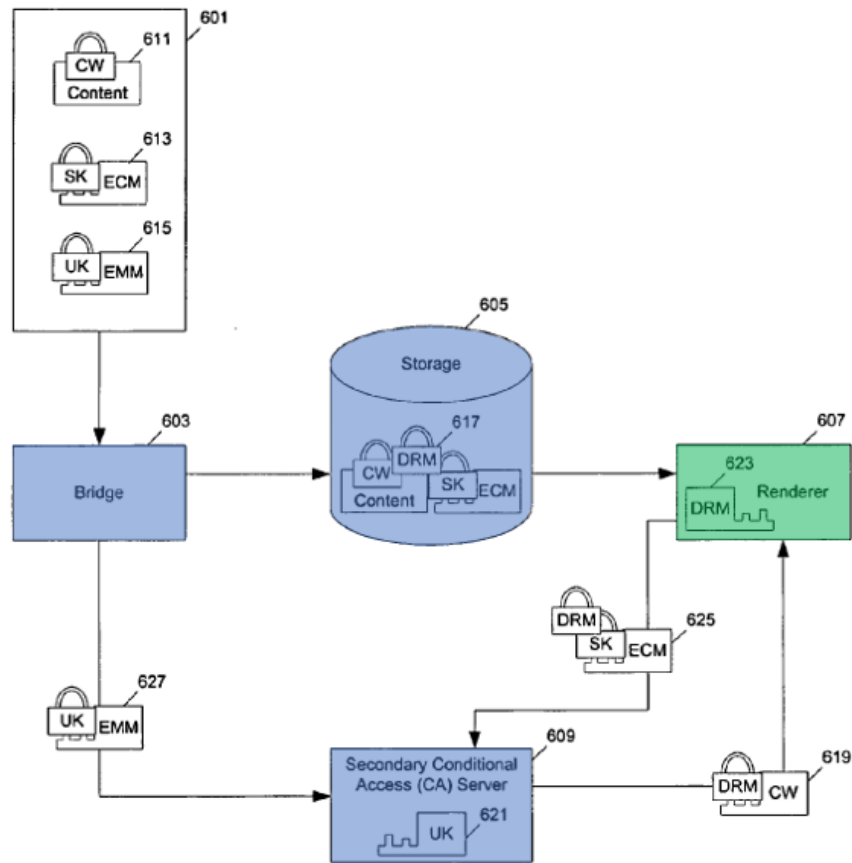


Fig. 11

See also EX1003 (“Wasilewski”), ¶¶31-42.

B. Prosecution History of the ’304

The ’304 issued from U.S. Application No. 13/612,663 (filed 2012-09-12) and claims to be a continuation of U.S. Application No. 11/007,116 (filed 2012-12-07), which issued as U.S. Patent No. 8,291,236. EX1002 (“’304FH”), 1-72; see also ’304, codes (22) and (63).

During prosecution, the Examiner rejected pending claims on the ground of nonstatutory obviousness-type double patenting over claims of the '236 and stated that the claims would be in condition for allowance pending submission and approval of a Terminal Disclaimer to overcome the double patenting rejection. '304FH, 92-98.

Applicant filed a Terminal Disclaimer in response. '304FH, 107-125.

The Examiner issued a Notice of Allowance shortly thereafter. '304FH, 129-137. The Examiner's reasons for allowance stated: "Nowhere in the prior art is found, alone, or in combination, other than via hindsight, the claim elements, at the time of the invention; serving to patently distinguish the invention from said prior art and thus this application is placed in condition for allowance. '304, 136. The '304 issued 2013-03-04. '304FH, 154. Wasilewski, ¶¶43-45.

C. Prosecution History of the '236

While the prosecution history of the '304 provides little detail about the nature of its claims' allowability (as discussed above), the prosecution history of the '236—to which the '304 claims priority and is terminally disclaimed—potentially sheds light as to the alleged merits of the claims over the prior art.

Specifically, the '236 issued from U.S. Application No. 11/007,116 (filed 2004-12-07), which was originally filed with 146 claims, 15 being independent. EX1015 ("236FH"), 1-129. In an Amendment dated 2012-05-01, preceding

allowance of the claims, each of the independent claims were amended, *inter alia*, to recite for the first time: “a first security domain,” “a second security domain,” client devices being of “the second conditional access server,” and “wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.” ’236FH, 556-599.

In the Notice of Allowance, the Examiner stated that “[n]owhere in the prior art is found, collectively ... ‘wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.’” ’236FH, 624. The ’236 issued 2012-10-16. ’236FH, 657.

Similar limitations are found in the Claims of the ’304. For example, the preamble of independent claim 5 recites, “wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust.” ’304, claim 5. Therefore, claims of the ’304 may have been deemed allowable over the prior art of record for the same reason. Wasilewski, ¶¶46-50.

V. LEVEL OF ORDINARY SKILL IN THE ART

On or before 2004-12-07, a person of ordinary skill in the art (“POSA”) 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. Wasilewski, ¶¶51-52.

VI. CLAIM INTERPRETATION

Claim terms subject to IPR are to be construed in accordance with their ordinary and customary meaning as understood by a POSA in light of the specification and prosecution history. 37 C.F.R. §42.100(b). Only terms necessary to resolve the controversy need to be construed. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

A. “content that is in an access controlled format specified by the second conditional access server”

Claim 5[b] recites “content that is in an access controlled format specified by the second conditional access server.” This limitation should be interpreted according to its ordinary and customary meaning: content that is in an access controlled format, the access controlled format specified by the second conditional access server. Wasilewski, ¶53.

In district court, the ’304 is asserted along with its parent, U.S. Patent No. 8,291,236 (“’236”). The ’236 includes similar but substantively different limitations. For example, claim 5 of the ’304 is compared with claim 130 of the ’236 below.

'304 Claim 5	'236 Claim 130
“content that is in an access controlled format specified by the second conditional access server”	“access controlled data that is in an access controlled format and that is at least partially derived from the security messages”

With respect to the '236, PO may be asserting that the limitation is to be interpreted as including an access controlled format derived from security messages. As Petitioner explains in its petitions directed to the '236, that interpretation misreads the plain language of the claims and is furthermore not supported by any written description. *See, e.g.*, IPR2024-01023, Petition §VI.A.

With respect to the '304, there can be no confusion—that same interpretation cannot be required in the claims. For example, claim 5 of the '304 does not recite any security messages, and so claim 5 cannot be interpreted to require that the access controlled format be derived from security messages. Nor does claim 5 limit, in any way, how or on what basis the second conditional access server has specified the access controlled format. Therefore, while PO may be alleging infringement of the '236 and the '304 in similar ways (*compare* EX1008 at 17-18 with EX1009 at 14-18), the claims should not be interpreted to have the same scope and certainly not the same incorrect scope. Wasilewski, ¶¶54-57.

VII. GROUNDS OF UNPATENTABILITY

This Petition is supported by the Declaration of Anthony J. Wasilewski, Ph.D., which describes the prior art's scope and content at the time of the '304.

- 17 -

In digital broadband delivery system (DBDS) 100, **headend 102** communicates with content providers 114 to obtain services such as broadcasts, video-on-demand, program guides, Internet access, etc., and to subsequently serve them to subscribers. Russ, 5:35-51, 9:26-10:24, 13:5-9. For example, **headend 102** services subscriber location 108(a) via **digital subscriber communication terminal (DSCT) 110** to provide service instances to **client-receiver 122**, such as one or more computers, televisions, VCRs, or other set-top terminals. Russ, 5:52-6:32, 6:51-61, 8:38-9:25, 14:1-3. Wasilewski, ¶¶59-60.

DSCT 110 registers with **headend 102** and is granted entitlements to service instances before receiving and accessing those service instances. Russ, 7:56-8:3. Thus, **headend 102** implements conditional access authority (CAA) logic to control access to DBDS 100 and, for example, grant entitlements to **DSCT 110** with control information and entitlement management messages (EMMs). Russ, 8:4-37, 10:48-50. **DSCT 110**, managing a local network at the subscriber location 108(a), can then provide permitted service instances to **client-receiver 122** with or out without further processing. Russ, 8:49-9:25, 16:32-42, 25:43-65. **DSCT 110** is the entitlement granting authority for client-receiver 122 and grants and deletes **client-receiver 122's** entitlements to service instances based on information received from **headend 102**. Russ, 17:61-18:40, 18:60-65; *see also* Fig. 2, 10:39-

41 (**headend 102** includes control system 232 and entitlement generator 236).
Wasilewski, ¶¶61-64.

The specific protected communications by which **DSCT 110** and **client-receiver 122** communicate is determined dynamically when **client-receiver 122** joins **DSCT 110's** network and provides an identification message containing device and hardware information. Russ, 3:17-20, 16:64-17:60, 20:12-20. Thus, depending on whether **client-receiver 122** is a laptop or a set-top, for example, **DSCT 110** communicates with **client-receiver 122** using different protocol and encryption schemes like secure sockets layer (SSL) or Digital Transmission Content Protection (DTCP) protocols. Russ, 17:4-14. Wasilewski, ¶62.

Because Russ discloses a first security server (**headend 102**) providing CA content (a service instance) and messages (EMMs and ECMs) to a CA server (**DSCT 110** receiving and processing the service instance, EMMs, and ECMs), and because the CA server (**DSCT 110**) communicates with clients (**client-receiver 122**) with a wholly separately negotiated encryption scheme (*e.g.*, DTCP used between **DSCT 110** and **client-receiver 122** but not between **headend 102** and **DSCT 110**), Russ discloses the conditional access server, method to process conditional access protection, and non-transitory machine readable medium as arranged in the claims of the '304. And, while anticipating features may sometimes be described as various “examples,” or “alternative” embodiment, or “another”

embodiment, such embodiments are not “distinct teachings that the artisan might somehow combine,” nor are they “not directly related to each other.” *Net MoneyIN, Inc. v VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (citing *In re Arkley*, 455 F.2d 586, 587 (C.C.P.A. 1972). Instead, the disclosures all directly relate to the same structures that make up Russ’s system (DBDS 100)— **headend 102**, **DSCT 110**, **client-receiver 122**—and represent non-limiting examples of implementations and not distinct, unrelated, embodiments. Russ therefore anticipates claims 5-6, 8, 16-17, and 19 of the ’304. Wasilewski, ¶¶71-123.

2. Claim Charts (5-6, 8)

'304	Russ (EX1005)
5[pre.i]². A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system	Russ discloses a non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause (e.g., software stored in memory and executed by a processor, secure element, and cryptographic device to implement logic steps) a client system in a second security domain to present content provided by a first conditional access server (e.g., causing client-receiver 122, in a second security domain with DSCT 110, to present service instances provided by headend 102, which implements conditional access authority logic with respect to DSCTs 110). Wasilewski, ¶¶71-80. Russ discloses a digital broadband distribution system (DBDS) 100 including a digital subscriber communication terminal (DSCT) 110 that provides, as a conditional access server in a second security domain, service instances to client-receiver 122, to which it “has the authority and capacity to grant and

² Regardless of whether the preamble is limiting, the prior discloses it.

'304	Russ (EX1005)
in a second security domain to present content provided by a first conditional access server	delete entitlements.” Russ, 5:35-39, 8:49-51, 17:61-18:51. DSCT 110 and client-receiver 122 are together in a second security domain (the “first” security domain will be shown with respect to claim 5[pre.ii] below) because they communicate securely with an encryption scheme that is specifically negotiated and established as between DSCT 110 and client-receiver 122 when client-receiver 122 joins DSCT 110’s network. Russ, 16:64-17:34, 20:12-24. Wasilewski, ¶¶72-77. The client-receiver 122 includes, <i>e.g.</i>, a video display to present a service instance to the user. Russ, 26:61-67. Wasilewski, ¶76. The services instance is locally received from DSCT 110, as discussed above, but is originally provided by headend 102 to DSCT 110. Russ, 7:58-8:3, 8:49-9:7, 18:8-18. Headend 102 is itself a conditional access server because it implements conditional access authority (CAA) logic to control access to service instances for a plurality of DSCTs 110. Russ, 8:8-22, 8:23-37, 10:48-65. Wasilewski, ¶78. Russ further discloses that the methods performed by the system, including by DSCT 110 and client-receiver 122, are implemented by an instruction execution system executing software stored in a memory. Russ, 3:23-40. Wasilewski, ¶79. <i>E.g.</i>, Regarding a non-transitory machine readable medium: • 3:23-40 (“The logic of the preferred embodiment(s) of the present invention can be <u>implemented in hardware, software, firmware, or a combination thereof</u>. In the preferred embodiment(s), <u>the logic is implemented in software or firmware that is stored in a memory and that is executed by a suitable instruction execution system</u>.”) Regarding a client system including client-receiver 122 in a second security domain with DSCT 110: • Fig. 1:

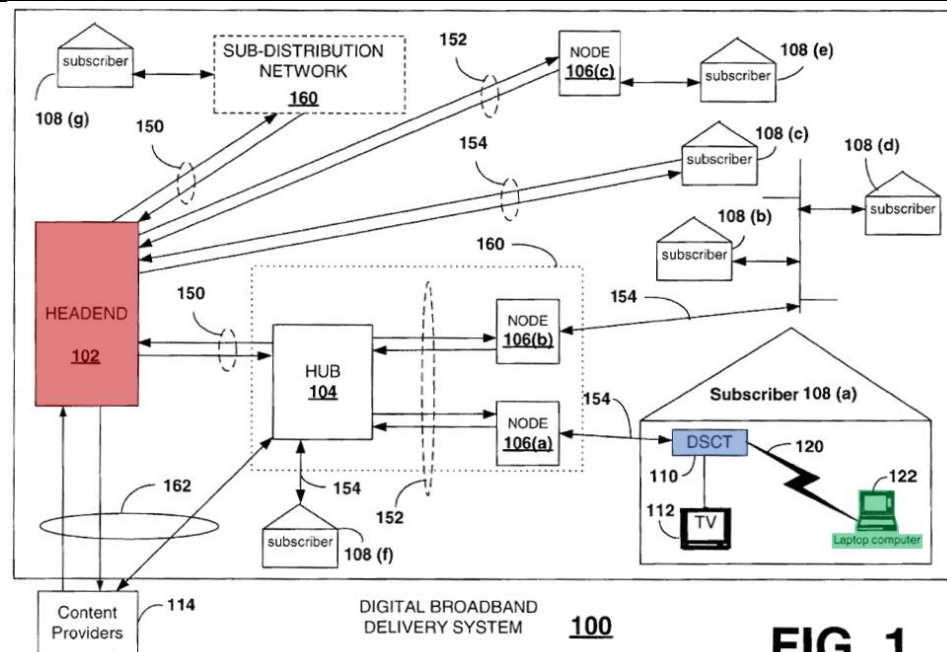


FIG. 1

- 5:35-39 (“Referring to FIG. 1, a digital broadband distribution system (DBDS) 100 includes, in one example among others, a headend 102, a plurality of hubs 104, multiple nodes 106, a plurality of subscriber locations 108, and a plurality of digital subscriber communication terminals (DSCTs) 110.”)
- 8:49-51 (“The client-receiver 122 is in two-way communication with the DSCT 110 and receives information and service instances therefrom.”)
- 16:64-17:14 (“The memory 310 includes logic for dynamic encryption scheme determination. Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium. For example, when the client-receiver 122 is a laptop, the encryption scheme may be different from when the client-receiver 122 is a PDA or set top. Non-limiting examples of dynamic encryption scheme determination logic include, but are not limited to, secure sockets layer (SSL) protocol,

'304	Russ (EX1005)
	<u>Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol.</u> These protocols and other dynamic encryption scheme determination logic known to those skilled in the art are intended to be within the scope of the invention.”) 17:15-34 (“Referring now to FIG. 4, the steps 400 are implemented for establishing private communication between the DSCT 110 and the client-receiver 122. In step 402, the DSCT 110 receives a client-receiver identification message from the client-receiver. The message is sent to the DSCT 110 when the client-receiver 122 discovers the local network maintained by the DSCT 110. The message includes device information such as hardware information about the client-receiver 122. In step 404, the processor 312 uses tables stored in memory 310 and the received client-receiver identification message to determine a classification for the client-receiver 122. <u>The processor 312 in negotiating an encryption scheme with the client-receiver 122 uses the classification of the client-receiver 122.</u> <u>In step 406, the processor 312 implements logic for negotiating an encryption scheme for the client-receiver 122. In the preferred embodiment, the encryption scheme is determined dynamically, when the client-receiver 122 is coupled to the local area network.”)</u> - Fig. 5:

'304	Russ (EX1005)
	<pre> graph TD 500((500)) --> 502[RECEIVE SERVICE REQUEST 502] 502 --> 504{IS C-R ENTITLED? 504} 504 -- NO --> 510[PROVIDE C-R WITH ENTITLEMENT 510] 510 --> 506{IS SERVICE ACCESSIBLE 506} 504 -- YES --> 506 506 -- NO --> 508[SEND REQUEST FOR SERVICE 508] 506 -- YES --> 512[PROVIDE C-R WITH SERVICE INSTANCE 512] 508 --> 512 </pre> FIG. 5 17:61-18:66 (“Referring to FIG. 5, steps 500 are implemented by processor 312 and the secure element 314. In step 502, <u>the DSCT 110 receives a request from the client-receiver 122 for a service instance.</u> The service instance is generally a user selected service instance such as a program selected by the user of the client-receiver 122. In another embodiment, the service instance is a service such as an Internet connection. In step 504, the secure element 312, which maintains a map of entitlements granted to the client-receiver, determines whether or not the client-receiver 122 is entitled to the requested service instance.... Some service instances are accessible to the DSCT 110 in response to requests of the user. For example, the DBDS 100 might include personal television, whereby the transmission of the service instance is controlled by the user, which means the transmission can be paused, rewound, etc., just like a

'304	Russ (EX1005)
	VCR. Another non-limiting example of a requested service instance includes pay-per-view programming. <u>If the selected service instance is not accessible at the DSCT 110, in step 508, the DSCT 110 sends a request for the service instance to the headend 102.</u> [...] In step 510, the client-receiver 122 is provided with the entitlement for the selected service instance. In the preferred embodiment, the secure element 314 generates the entitlement for the selected service instance and provides the entitlement to the client-receiver 122. Typically, the secure element 314 generates an EMM, which includes the entitlement, and sends the entitlement to the client-receiver 122 via the communication link 120. In this embodiment, the DSCT 110 acts as an entitlement granting authority for the client-receiver 122. <u>The DSCT 110 has the authority and capacity to grant and delete entitlements to the client-receiver 122 for the service instance.</u> [...] The secure element 314 of the DSCT 110 then processes the EMM and provides the entitlement to the client-receiver 122. <u>In step 512, the selected service instance is provided to the client-receiver 122.”)</u> • 20:12-24 (“When the processor 312 determines to encrypt the service instance, then in step 612, the service instance is provided to the cryptographic device 318. <u>The cryptographic device 318 encrypts the service instance using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122.</u> Typically, the secure element 314 provides the cryptographic device 318 with the encryption keys used by the cryptographic device 318 to encrypt the service instance. [...] <u>In step 614, the client-receiver interface 320 transmits the service instance to the client-receiver 122.”)</u>

Regarding the **client-receiver 122** presenting content:

- 26:61-67 (“The cryptographic device 912 decrypts the service instance using control words provided by the secure element 908 and sends the decrypted service instance to the output port 916. Typically, a user device (not shown) such as a video display or a speaker is coupled to output port 916 for providing the service instance to the user.”)

Regarding **headend 102** being a first conditional access server and providing content:

- Fig. 1:

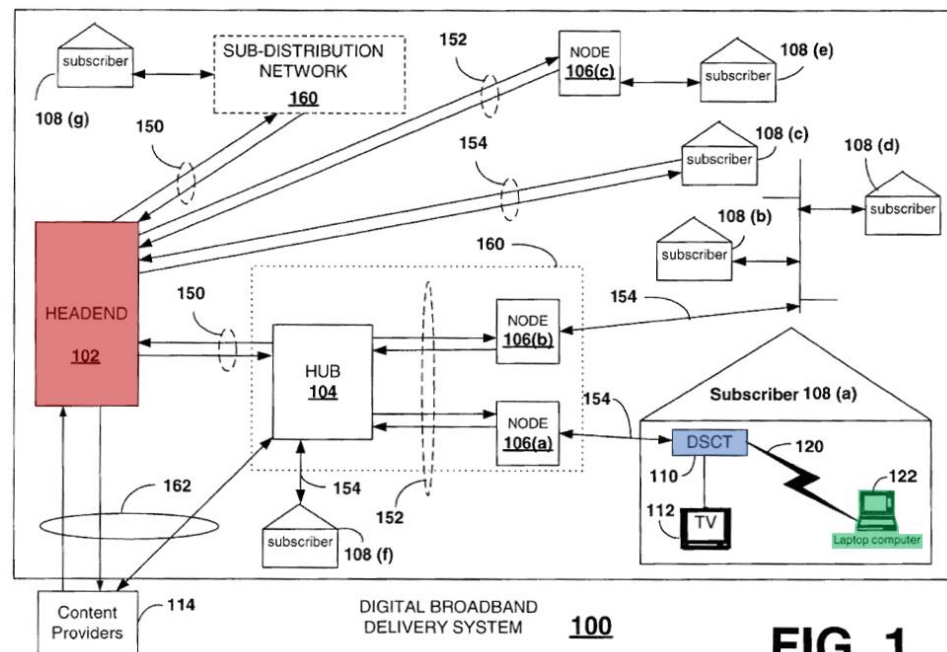


FIG. 1

- 7:56-8:3 (“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

'304	Russ (EX1005)
	the trusted public keys of the DSCT 110 with its own trusted public key. This is accomplished by having the manufacturer of the DSCT 110 digitally sign two messages, which include the new trusted public key, for the DSCT 110 and then sending the two messages to the DSCT 110.”) 8:8-22 (“<u>There is conditional access authority (CAA) logic implemented in the headend 102 that the access controlling authority uses for controlling access to the DBDS 100. The conditional access authority sends the DSCT 110 a secure message such as an entitlement management message (EMM), which is digitally signed by a private key of the conditional access authority.</u> For the purposes of this disclosure, a secure message includes, as a non-limiting example, a message that has been digitally signed by the sender so that the recipient can verify the source of the message and verify that the content of the received message was not tampered with nor corrupted in transmission. The content of a secure message may be encrypted when the sender wants to make the content private or the content can be transmitted without encryption.”) 8:23-37 (“In the preferred embodiment, the private key of the conditional access authority corresponds to one of the trusted public keys of the DSCT 110. The DSCT 110 authenticates the EMM using the trusted public key of the conditional access authority and acts upon the EMM only if the EMM is authenticated as having come from the conditional access authority. <u>Among other things, the conditional access authority uses EMMs to instruct the DSCT 110 to allocate a portion of its memory for entitlement information related to a service instance provided by an entitlement agent and to provide the DSCT 110 with the public key for an entitlement agent.</u> The memory of the DSCT 110 is partitionable so that it can contain entitlement information for service instances from multiple entitlement agents and public keys from each of

'304	Russ (EX1005)
	those entitlement agents.”) 10:48-65 (“<u>The CAA 234 is used by the access controlling authority to enable DSCTs 110 to receive entitlements for service instances.</u> The CAA 234 receives EMM templates from the EMM generator 238 and uses the EMM template to create an EMM. To create an EMM, the CAA 234 includes a message content and an authentication token in the EMM template. The CAA 234 determines whether the message content should be encrypted, and if so, the CAA 234 encrypts the message content using the public key of the recipient of the EMM, which is retrieved from the database 240. The authentication token of an EMM is generally a one-way hash digest of the message content that has been digitally signed by the private key of the CAA 234. In the preferred embodiment, the recipient, i.e., the DSCT 110, implicitly trusts any EMM that has an authentication token from the CAA 234 because the CAA 234 signs the hash digest with the private key that corresponds to one of the trusted public keys stored in the DSCT 110.”) 17:61-18:66 (<i>see above</i>) See also: 3:11-22, 4:21-39, 8:38-9:7, 16:13-26, 19:7-42, 24:3-7, 24:37-38
5[pre.ii]. wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication	Russ discloses that the first conditional access server (e.g., headend 102) has authenticated a client device of the first conditional access server (e.g., DSCT 110) through a first authentication process using a first root of trust (e.g., 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, and then providing a new trusted DBDS 100 public key to the DSCT 100; DBDS 100 registers DSCT 100 as a client to receive service instances) for a first security domain (e.g., headend 102 implements conditional access authority (CAA) logic to control access to service instances for a plurality of DSCTs 110; headend 102

'304	Russ (EX1005)
process using a first root of trust for a first security domain and	and DSCT 110 exchange public keys to establish and conduct secure communications with each other). Wasilewski, ¶¶81-85. Russ discloses that when a DSCT 110 connects to the DBDS, headend 102 authenticates the DSCT 110 by verifying that the DSCT 110's unique serial number is in a database of serial numbers and corresponding keys that have been certified by the manufacturer. Russ, 7:21-39, 7:56-8:3, 10:39-47. DSCT 110, once registered with the DBDS 100 through headend 102, is a client of the headend 102 that can receive service instances and entitlements. Russ, 7:56-8:3. Wasilewski, ¶¶82-83. "Root of trust" is not explicitly defined in the '304, but in context, a POSA would have recognized it as at least including hardware, software, and/or firmware-based systems for establishing trustworthy identities of components or entities, as in Russ. Wasilewski, ¶83. DSCT 110 and other DSCTs 110, having registered with headend 102 so that it may receive conditional access service instances and entitlements, and having exchanged keys for secure communications, are in a first security domain with headend 102. Russ, 6:62-7:6, 8:8-22. This is a "first" security domain different from the "second" security domain established with the dynamically determined encryption scheme between DSCT 110 and client-receiver 122, discussed above with respect to claim 5[pre.i]. Wasilewski, ¶84. <i>E.g.,</i> Regarding DSCT 110 and headend 102 being in a first security domain: • 6:62-7:6 ("Secure communication between the headend 102 and the DSCTs 110 is preferably accomplished using pairs of asymmetrical keys known to those skilled in the art, such as Rivest, Shamir, & Adleman (RSA) public key encryption technology. [...] <u>The headend 102 and the DSCT 110 can securely communicate after they have exchanged public keys.</u>") • 8:8-22 ("<u>There is conditional access authority (CAA) logic implemented in the headend 102 that the access</u>

'304	Russ (EX1005)
	<u>controlling authority uses for controlling access to the DBDS 100. The conditional access authority sends the DSCT 110 a secure message such as an entitlement management message (EMM), which is digitally signed by a private key of the conditional access authority. For the purposes of this disclosure, a secure message includes, as a non-limiting example, a message that has been digitally signed by the sender so that the recipient can verify the source of the message and verify that the content of the received message was not tampered with nor corrupted in transmission. The content of a secure message may be encrypted when the sender wants to make the content private or the content can be transmitted without encryption.”)</u> Regarding headend 102 authenticating DSCT 110 using a first root of trust: • 7:21-39 (“<u>In the preferred embodiment, when the DSCT 110 is manufactured it is assigned a serial number, and it is provided with its own private key-public key pair and with a public key of an access controlling authority. The keys are provided to the DSCT 110 in a secure manner and stored in a protected memory in the DSCT 110. The manufacturer of the DSCT maintains a database that includes the public keys and the serial numbers of each of the DSCTs 110 that the manufacturer produces. Each DSCT 110 in the DBDS 100 has a unique serial number, and the serial number, which can be the MAC address of the DSCT 110, is used for addressing messages to the DSCT 110. The manufacturer provides a copy of the public key and the serial number of each DSCT 110 in the DBDS 100 to the operator of the DBDS 100. In that case, the 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. The operator of the DBDS 100 maintains its database of public keys and serial numbers of each DSCT 110 in the DBDS 100.”)</u>”) • 7:40-55 (“<u>In the preferred embodiment, the DSCT 110 is</u>”)

'304	Russ (EX1005)
	<u>provided with multiple public keys during its manufacture. Because these keys were given to the DSCT 110 during its manufacture in a secure fashion, the DSCT 110 implicitly trusts these keys. The DSCT 110 trusts any message that is signed by a private key corresponding to one of these trusted public keys. At least one of the trusted public keys can be replaced by a different public key, which then becomes a trusted public key. To replace a trusted key the DSCT 110 receives at least two messages with a new trusted public key included therein. A private key corresponding to one of the trusted public keys that are not being replaced signs each of the messages. The DSCT 110 uses its trusted public keys to verify that the messages were signed by one of the corresponding private keys. The DSCT 110 only replaces one of its trusted public keys when the message is verified.”)</u> 7:56-8:3 (<u>“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. This is accomplished by having the manufacturer of the DSCT 110 digitally sign two messages, which include the new trusted public key, for the DSCT 110 and then sending the two messages to the DSCT 110.”)</u> 10:39-47 (<u>“The control system 232 includes database 240 and logic for conditional access authority (CAA) 234, entitlement generator 236 and EMM generator 238. Database 240 includes, among other things, the serial numbers and public keys of the DSCTs 110 of DBDS 100. The EMM generator 238 uses database 240 to generate</u>

'304	Russ (EX1005)
	individually addressable EMM templates. The EMM generator 238 can also generate EMM templates for multiple DSCTs 110 and/or global EMM templates.”) See also: • 8:4-11, 8:23-37, 10:48-65
5[pre.iii]. wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:	Russ discloses that a second conditional access server (<i>e.g.</i>, DCST 110 is a second conditional access server to client-receiver 122) is configured to substitute the first security domain with the second security domain (<i>e.g.</i>, DCST 110 receives the service instance from headend 102, decrypts the service instance, then encrypts the service instance with an encryption scheme specifically negotiated between DCST 110 and client-receiver 122) for the clients under the second root of trust (<i>e.g.</i>, client-receiver 122 and other client-receivers 122 are under a second root of trust established with DCST 110 via DTCP authentication and based on an Authentication and Key Exchange (AKE) using DTLA licensed certificates). Wasilewski, ¶¶86-94. As discussed above for claim 5[pre.i], DSCT 110 is a conditional access server to client-receiver 122 in a second security domain, and service instances received at client-receiver 122 are transmitted from headend 102 to DSCT 110 to client-receiver 122. Russ discloses that DSCT 110 decrypts service instances received from headend 102 and then re-encrypts the service instances for transmission to client-receiver 122. Russ, 8:49-9:7, 15:46-54, 19:50-20:19. Between headend 102 and DSCT 110, a service instance may be encrypted/decrypted by a multi-session key and CA control words (<i>see</i> Russ, 11:37-61, 13:12-34), while the re-encrypted service instance is protected by DTCP encryption between DSCT 110 and client-receiver 122 (<i>see</i> Russ, 16:64-17:34; <i>see</i> discussions of claims 5[pre.i]-[pre.ii] above). DSCT 110 therefore substitutes the first security domain using CA with the second security domain using DTCP. Wasilewski, ¶¶87-90. A POSA would have recognized that DTCP protocols include

'304	Russ (EX1005)
	authentication and key and certificate exchange procedures that ensure communications are protected. <i>See, e.g.</i>, EX1010 (US 2002/0025042), [0009] (describing an authentication and key exchange procedure between transmitting and receiving devices under DTCP); EX1011 (US 2005/0027984), [0053] and [0107] (describing device identification numbers embedded in a device certificate issued by a licensing institution such as the DTLA), [0139]-[0143] and Fig. 17 (describing a “DTCP communication sequence” including an authentication and key exchange prior to transmission of content). Client-receiver 122 is therefore under a second root of trust with DSCT 110, with the different “first” security domain and root of trust through authentication being between headend 102 and DSCT 110 as discussed for claim 5[pre.ii] above. Wasilewski, ¶¶91-93. <i>E.g.</i>, Regarding the first security domain including headend 102 and DSCT 110: • 11:37-46 (“The entitlement generator 236 generates encryption information and the entitlements of the DSCTs for the service instances. The entitlement generator 236 provides the encryption information to the multi-transport stream transceiver 228, which generates control words therefrom for encrypting the service instances. <u>In the preferred embodiment, the encryption information is a multi-session key (MSK), which has a relatively long life, such as days, weeks, or months. The MSK is transmitted to the DSCTs 110 in EMMs created by the entitlement generator 236.</u>”) • 13:12-34 (“<u>The multi-transport stream transmitter/receiver 228 uses the MSK from the control system 232 to encrypt service instances.</u> The multi-transport stream transmitter/receiver 228 includes a counter that produces a numerical value every couple of seconds or so and an encryptor. <u>The encryptor uses the MSK to encrypt the counter value to produce a control word. The control word is used by the encryptor as a key for encrypting a portion of the service instance.</u>”)

'304	Russ (EX1005)
	The multi-transport stream transmitter receiver 228 includes the counter value in an entitlement control message (ECM), which is multiplexed into the output transport stream 242. [...] <u>Only DSCTs that have the MSK will be able to encrypt the counter value of the ECM to generate the control word that decrypts the service instance.</u>") Regarding the second security domain including DSCT 110 and client-receiver 122: • 16:64-17:14 ("The memory 310 includes logic for dynamic encryption scheme determination. <u>Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium. For example, when the client-receiver 122 is a laptop, the encryption scheme may be different from when the client-receiver 122 is a PDA or set top. Non-limiting examples of dynamic encryption scheme determination logic include, but are not limited to, secure sockets layer (SSL) protocol, Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol. These protocols and other dynamic encryption scheme determination logic known to those skilled in the art are intended to be within the scope of the invention.</u>") • 17:15-34 (see claim 5[pre.i]) Regarding DSCT 110 substituting the first security domain for the second security domain: • 15:46-54 ("When the DSCT 110 is entitled to the selected service instance, the secure element 314 provides the cryptographic device 318 with the control word used for decrypting the selected service instance. <u>The cryptographic device 318 decrypts the selected service instance using the control word from the secure element 314 and the</u>

decrypted service instance is sent to the output port 322. The manner in which the secure element 314 determines whether the DSCT 110 is entitled is described in detail hereinbelow.”)

- Fig. 6

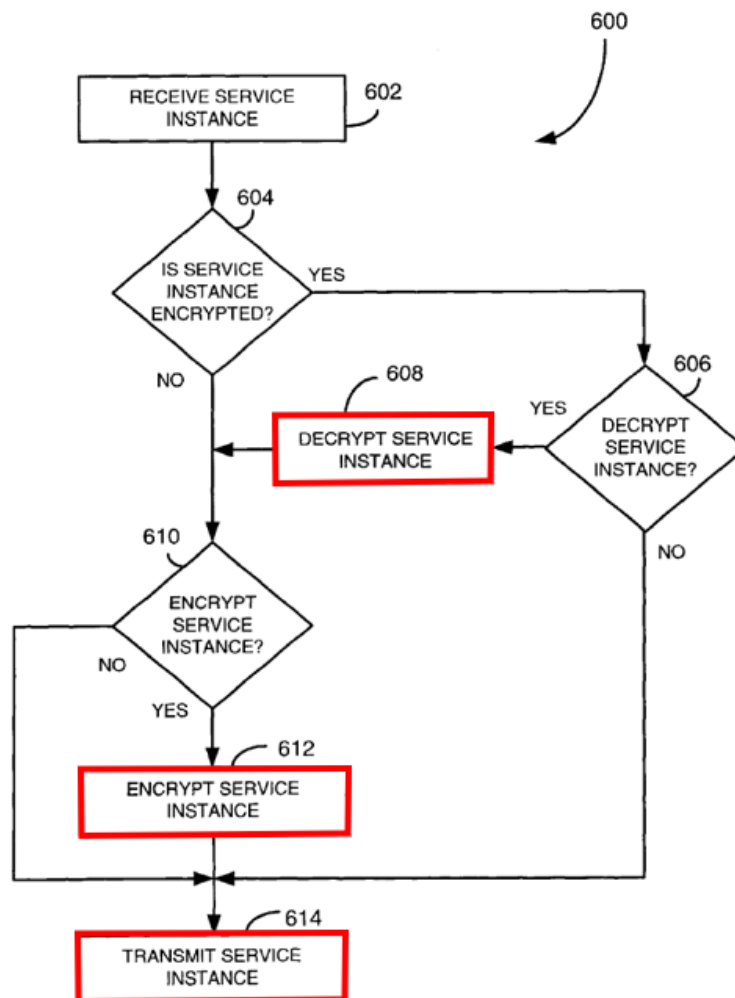


FIG. 6

- 19:50-20:19 (“In step 604, the processor 312 uses system tables to determine whether or not the service instance is encrypted. [...]”)

On the other hand, when the processor 312 determines to decrypt the service instance, the processor 312 instructs the tuner to send the service instance to the cryptographic

'304	Russ (EX1005)
	device 318. <u>In step 608, the cryptographic device 318 decrypts to the service instance using the control word(s) provided by the secure element 314.</u> <u>In step 610, the processor 312 determines an encryption scheme for the selected service instance. [...]</u> <u>When the processor 312 determines to encrypt the service instance, then in step 612, the service instance is provided to the cryptographic device 318. The cryptographic device 318 encrypts the service instance using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122. Typically, the secure element 314 provides the cryptographic device 318 with the encryption keys used by the cryptographic device 318 to encrypt the service instance.”)</u> See also: • 8:49-9:7, 23:47-67
5[a]. receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication	Russ discloses receiving, at a second conditional access client of the second conditional access server (<i>e.g.</i>, receiving at client-receiver 122, which is a client of second conditional access server DSCT 110), an authentication through a second authentication process (<i>e.g.</i>, DSCT 110 authenticates client-receiver 122 through DTCP protocols) which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust (<i>e.g.</i>, DTCP authentication is 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 root of trust’s use of serial numbers and keys between the headend 102 and DSCT 110 discussed in claim 5[pre.iii]). Wasilewski, ¶¶95-97. Russ discloses that protocols for communication between DSCT 110 and client-receiver 122 are determined dynamically, for example when client-receiver 122 joins DSCT 110’s network and identifies itself. <i>See</i> discussion of

'304	Russ (EX1005)
process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and	claim 5[pre.i] above. DSCT 110 and client-receiver 122 may thus follow DTCP protocols. Russ, 16:64-17:14. As further discussed for claim 5[pre.iii] above, a POSA would have recognized that DTCP protocols include authentication and key and certificate exchange procedures that ensure communications are protected. <i>See, e.g.</i>, EX1010 (US 2002/0025042), [0009]; EX1011 (US 2005/0027984), [0053], [0107], [0139]-[0143], Fig. 17. Communications 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. Wasilewski, ¶96. <i>E.g.</i>, Russ discloses: • 16:64-17:14 (<i>see</i> claim 5[pre.i] above)
5[b] receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.	Russ discloses receiving, at the second conditional access client, content (<i>e.g.</i>, client-receiver 122 receives a service instance from DSCT 110) that is in an access controlled format specified by the second conditional access server (<i>e.g.</i>, DSCT 110 determines the encryption scheme used for communications between DSCT 110 and client-receiver 122, using, <i>e.g.</i>, a DTCP access controlled format; DSCT 110 formats the service instance for transmission using the determined encryption scheme) in the second security domain, the second conditional access client being in the second security domain (<i>e.g.</i>, DSCT 110 and client-receiver 122 are in the second security domain, as discussed for claim 5[pre.i] above). Wasilewski, ¶¶98-103. Russ discloses that protocols for communication between DSCT 110 and client-receiver 122 are determined dynamically, for example when client-receiver 122 joins DSCT 110's network and identifies itself. <i>See</i> discussion of claim 5[pre.i] above. DSCT 110 may also determine the encryption scheme based on other factors, including an amount of content being delivered, a user input, or a minimum desired level of security. Russ, 17:34-47. DSCT 110 may thus determine to use an encryption scheme based on DTCP protocols. Russ, 16:64-17:34. Wasilewski, ¶99.

'304	Russ (EX1005)
	When DSCT 110 transmits service instances to client-receiver 122, DSCT 110 encrypts the service instance using the dynamically determined encryption scheme—<i>e.g.</i>, formatting the data according to DTCP protocols. Russ, 20:12-24. Wasilewski, ¶¶100-101. <i>E.g.</i>, Regarding DSCT 110 specifying the access controlled format: • 16:64-17:14 (<i>see</i> claim 5[pre.i] above) • 17:15-34 (“Referring now to FIG. 4, the steps 400 are implemented for establishing private communication between the DSCT 110 and the client-receiver 122. In step 402, the DSCT 110 receives a client-receiver identification message from the client-receiver. The message is sent to the DSCT 110 when the client-receiver 122 discovers the local network maintained by the DSCT 110. The message includes device information such as hardware information about the client-receiver 122. In step 404, the processor 312 uses tables stored in memory 310 and the received client-receiver identification message to determine a classification for the client-receiver 122. The processor 312 in negotiating an encryption scheme with the client-receiver 122 uses the classification of the client-receiver 122. <u>In step 406, the processor 312 implements logic for negotiating an encryption scheme for the client-receiver 122. In the preferred embodiment, the encryption scheme is determined dynamically, when the client-receiver 122 is coupled to the local area network.”)</u> • 17:34-47 (“<u>In an alternative embodiment, the encryption scheme is determined dynamically responsive to dynamic changes in the local area network, such as the amount of content delivered to the client-receiver 122, or responsive to user input.</u> For example, the user of the client-receiver 122 might desire a different level of encryption than the one that was negotiated. In that case, user selects the different level, higher or lower, and the client-receiver 122

in the DSCT 110 negotiate a new level of security based upon the input of the user. However, in the preferred embodiment, the DSCT 110 can override the input of the user when negotiating the encryption scheme, so as to maintain at least a predetermined minimum level of security.")

Regarding **client-receiver 122** receiving content in the access controlled format from **DSCT 110**:

- Fig. 6

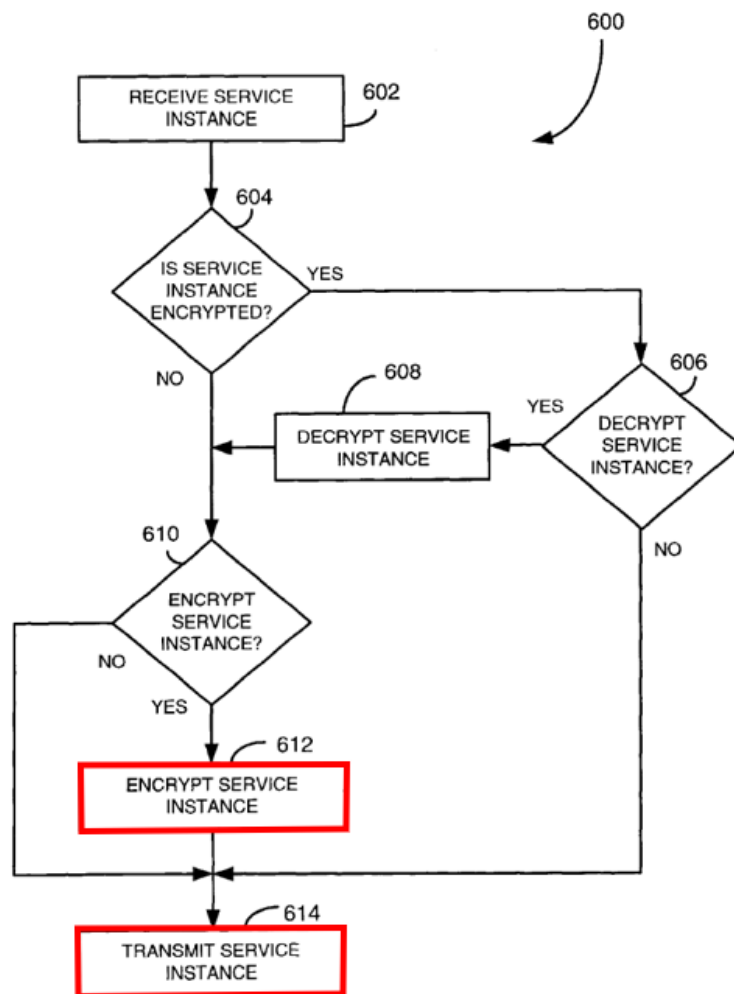


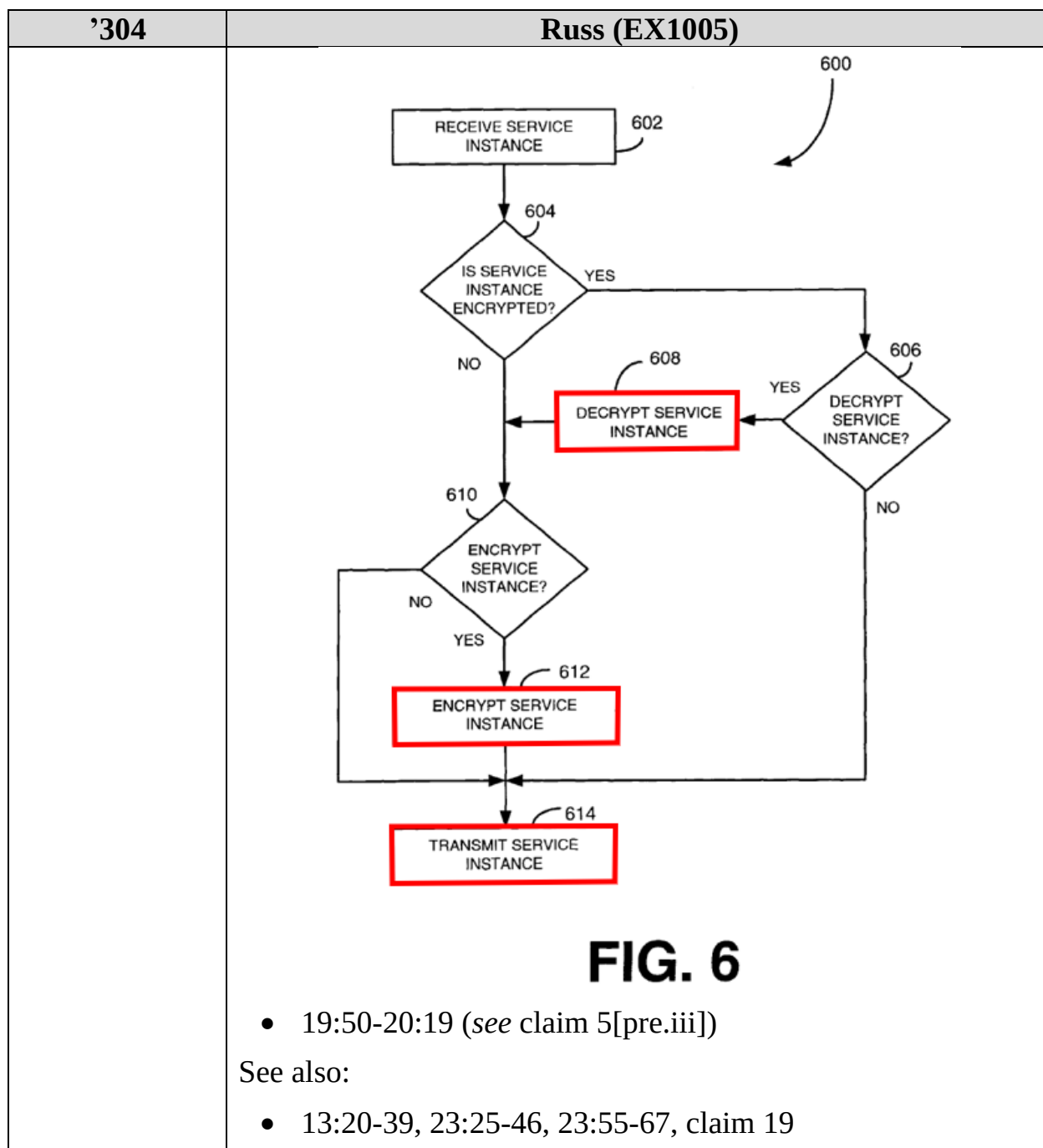
FIG. 6

'304	Russ (EX1005)
	• 20:12-24 (see claim 5[pre.i]) See also: • 3:17-20, 17:15-23, 25:17-25 Additionally, to the extent PO argues that the access controlled format must be derived from security messages (which cannot reasonably be required in the '304, see §VI.A)—Russ discloses the access controlled format partially derived from security messages (e.g., headend 102 transmits an EMM to DSCT 110 dictating the encryption scheme for communications with client-receiver 122). • 25:17-22 (“<u>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. In that case, the headend 102 determines the encryption scheme used to communicate information between the DSCT 110 and the client-receiver 122.</u>”) • See also 16:31-63, 19:7-27, 25:22-25.
6. The medium in claim 5, wherein the second conditional access client does not have a user key representing a subscriber of the first security system.	Russ discloses that the second conditional access client does not have a user key representing a subscriber of the first security system (e.g., client-receiver 122 generates control words using secrets shared with DSCT 110 and therefore has a user key representing a subscriber of DSCT 110; client-receiver 122 does not have a user key as a subscriber of headend 102). Russ discloses that secrets are shared between DSCT 110 and client-receiver 122 for client-receiver 122 to, e.g., generate control words to decrypt service instances. Russ, 20:47-53, 26:16-28. Client-receiver 122 does not have or require shared secrets with headend 102. See also Russ, 8:49-9:7 (DSCT 110 decrypts information from headend 102 and re-encrypts them for client-receiver 122. Wasilewski, ¶¶104-107. E.g., Regarding client-receiver 122 sharing secrets with DSCT 110 but not with headend 102: • 20:47-53 (“<u>The secrets 708 are secrets that are shared</u>

'304	Russ (EX1005)
	<u>between the DSCT 110 and the client-receiver 122. In the preferred embodiment, the secrets 708 are used for, among other things, encrypting service instances provided to the client-receiver 122, generating authentication tokens for messages transmitted to the client-receiver 122 and authenticating messages from the client-receiver 122.”)</u> 26:16-28 (“In the preferred embodiment, the secure element 908 includes a processor (not shown) and a memory (not shown) that are included in tamper resistant packaging. Among other things, the secure element 908 generates secure messages; processes received EMMs, and generates control words for the cryptographic device 912. <u>The secure element 908 includes entitlements granted to the client-receiver 122, secrets for authenticating messages and generating control words, and keys such as a private key-public key pair of the client receiver 122 and other public keys. The other public keys include trusted public keys, the public key of the conditional access authority 234 and the public key of the DSCT 110.”)</u> See also: 8:49-9:7
8. The medium in claim 5, wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.	Russ discloses that the content comprises a result of descrambling data (e.g., DSCT 110 encrypts and transmits a decrypted service instance to client-receiver 122) scrambled by a conditional access system of the first security system (e.g., the service instance was scrambled by headend 102). Wasilewski, ¶¶108-111. DSCT 110 receives service instances from headend 102. Russ, 7:56-58. Prior to transmission to DSCT 110, service instances are encrypted with control words and/or with a Digital Video Broadcasting (DVB) Common Scrambling technique. Russ, 12:47-13:19. Wasilewski, ¶110. DSCT 110 descrambles received service instances, encrypts descrambled service instances according to the encryption scheme determined between DSCT 110 and client-receiver 122, and transmits the encrypted descrambled service instances

'304	Russ (EX1005)
	to client-receiver 122. Russ, Fig. 6, 15:46-54, 16:64-17:14, 19:50-20:19. Wasilewski, ¶109. <i>E.g.</i>, Regarding data having been scrambled by headend 102: • 7:56-58 (“Before the <u>DSCT 110 receives</u> and accesses <u>service instances from the headend 102</u>, the DSCT 110 is registered with the headend 102 and entitled to the service instances.”) • 12:47-13:19 (“In the preferred embodiment, <u>the multi-transport stream receiver-transmitter 228 is adapted to encrypt content prior to modulating and transmitting the content. Typically, the content is encrypted using a cryptographic algorithm such as the Data Encryption Standard (DES) or triple DES (3DES), Digital Video Broadcasting (DVB) Common Scrambling or other cryptographic algorithms or techniques known to those skilled in the art. [...]</u> It is to be understood that for the purposes of this disclosure a “program” extends beyond a conventional television program and that it includes video, audio, video-audio programming and other forms of services and digitized content. “Entitled” DSCTs 110 are allowed to use the decryption information to decrypt encrypted content, details of which are provided hereinbelow. <u>The multi-transport stream transmitter/receiver 228 uses the MSK from the control system 232 to encrypt service instances. The multi-transport stream transmitter/receiver 228 includes a counter that produces a numerical value every couple of seconds or so and an encryptor. The encryptor uses the MSK to encrypt the counter value to produce a control word. The control word is used by the encryptor as a key for encrypting a portion of the service instance.”)</u> Regarding descrambling the scrambled data and encrypting the result for client-receiver 122: • 15:46-54 (“<u>The cryptographic device 318 decrypts the</u>

'304	Russ (EX1005)
	<u>selected service instance using the control word from the secure element 314 and the decrypted service instance is sent to the output port 322.”)</u> • 16:64-17:14 (“The memory 310 includes logic for dynamic encryption scheme determination. <u>Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium. [...]</u> Non-limiting examples of dynamic encryption scheme determination logic include [...] Digital Transmission Content Protection (DTCP) [...].”) • Fig. 6



3. Claim Charts (16-17, 19)

Independent claim 16 and its dependent claims are directed to method steps (and related structures) that are substantially similar to the functions and steps of independent machine readable medium claim 5 and its dependent claims. The

claims are therefore disclosed for the same reasons identified above and as identified in the chart below. Wasilewski, ¶¶112-119.

'304	Russ (EX1005)
16[pre.i]. A method at a client system in a second security domain to present content provided by a first conditional access server	<i>See claim 5[pre.i] (disclosing a method wherein a data processing system causes “a client system in a second security domain to present content provided by a first conditional access server”).</i>
16[pre.ii]. wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and	<i>See claim 5[pre.ii].</i>
16[pre.iii]. wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client	<i>See claim 5[pre.iii].</i>

'304	Russ (EX1005)
devices under a second root of trust, the method comprising:	
16[a]. receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and	See claim 5[a].
16[b]. receiving, at the second conditional access client, content that is in an access	See claim 5[b].

'304	Russ (EX1005)
controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.	
17. The method in claim 16, wherein the second conditional access client does not have a user key representing a subscriber of the first security system.	See claim 6.
19. The method in claim 16, wherein the content comprises a result of descrambling data scrambled by a conditional access system of the first security system.	See claim 8.

B. Ground 2: Claims 5-6, 8, 16-17, and 19 are Obvious Over Russ

Russ anticipates claims 5-6, 8, 16-17, and 19 as discussed in §VII.A above. Wasilewski, ¶¶121-122. To the extent PO argues that various features of Russ that are identified in the charts above are from distinct and unrelated embodiments—and would allegedly preclude a finding of anticipation—Russ further teaches that its disclosed features are combinable, and a POSA would have thus found the claims obvious as well.

As discussed in §VII.A.1 above, the various examples and embodiments disclosed in Russ are directly related to each other as non-limiting examples of implementations of the same system elements: **headend 102**, **DSCT 110**, **client-receiver 122**. As Russ explains, the “examples ... are merely examples among other possible examples,” described “embodiments ... are merely possible non-limiting examples of implementations, merely setting forth a clear understanding of the principles of the inventions,” and “changes, modifications, or alternations to the invention as described may be made” without “depart[ing] from the spirit of the invention.” Russ, 2:52-54, 27:8-20. A POSA would have therefore 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. Wasilewski, ¶123.

Accordingly, in light of the structures and functions identified in the claim charts in §VII.A.2-A.3 above, which also apply here, claims 5-6, 8, 16-17, and 19 are obvious over Russ. Wasilewski, ¶124.

C. Ground 3: Claims 7 and 18 are Obvious Over Russ in view of Robert

1. Overview: Robert

Robert describes a method for conditional access (CA) to digital rights management (DRM) conversion, which are “seemingly incompatible and different content protection systems,” allowing for consumption of content in accordance with a content protection scheme that is different than a content protection scheme with which it originated. EX1006 (“Robert”), Abstract, 2:23-33, 6:17-30. Robert discloses transmitting and consuming content across the systems by transcribing content protection information from one syntax to the other. Robert, 6:26-30. Wasilewski, ¶¶65-67.

Fig 5 below shows exemplary steps for producing a DRM license according to content protection information for a CA protection scheme. Robert, 12:4-15.

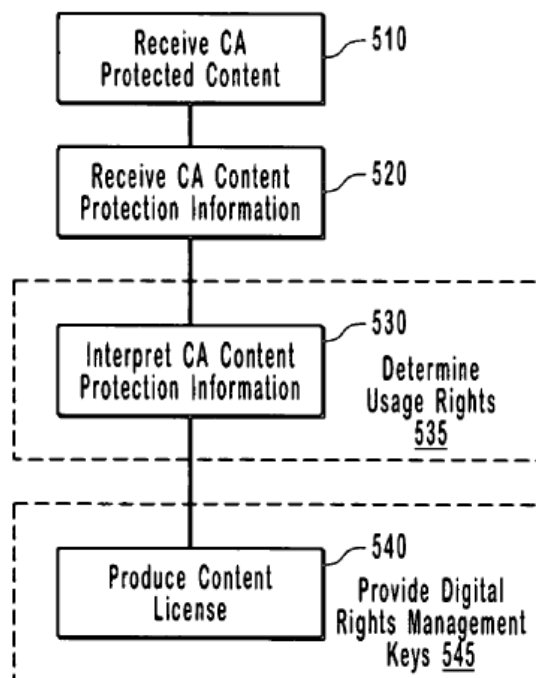


Fig. 5

Steps include interpreting the 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. Robert, 12:16-26. Wasilewski, ¶66.

In addition to the broad steps outlined above, variations include transcribing content, including control words (CWs) and keys in the DRM license, decrypting and re-encrypting the CA content with DRM methods, and performing such steps at different times and on different devices. Robert, 6:26-59. Wasilewski, ¶67.

2. Motivation: Russ in view of Robert

Russ and Robert are in the same field as the '304—*e.g.*, content protection schemes. '304, 1:9-2:55. *See* Russ, Abstract (encryption and re-transmission of service instances from a headend to a networked client-receiver), 1:5-2:14 (entitlements in conditional access systems); Robert, Abstract, 1:12-2:19 (interfacing content protection schemes). Wasilewski, ¶68.

As explained in §VII.A above, Russ discloses a system in which **headend 102** provides service instances and entitlements to service instances to **DSCT 110**, and **DSCT 110**, managing its own local network at a subscriber location, serves a **client-receiver 122** and provides it with service instances and entitlements communicated with an encryption scheme dynamically determined for use between **DSCT 110** and **client-receiver 122** only. However, Russ leaves to the POSA what known method to use for protected communication between **DSCT 110** and **client-receiver 122** and does not explicitly recite all details—for example what specific information or control words client-receiver 122 uses to decrypt service instances (*e.g.*, with respect to claims 7 and 18). Robert teaches implementation examples for providing content and content protection information across different content protection schemes. It would have been obvious to a POSA to transmit control words from **DSCT 110** to **client-receiver 122** in Russ, as taught by Robert, for the reasons below. Wasilewski, ¶125.

Regarding claim 7 and 18, Russ discloses that **client-receiver 122** decrypts service instances by generating control words. Russ, 26:16-28, 26:54-67. However, Russ leaves implementation details to the POSA regarding, for example, how **client-receiver 122** generates control words and/or whether **DSCT 110** transmits control words, control word indicators, counters, or ECMs to **client-receiver 122**—though Russ discloses that communications between **DSCT 110** and **client-receiver 122** are the negotiated protocols and encryption depending on **client-receiver 122's** hardware. Russ, 16:64-17:60, 20:12-17, 26:34-37, 26:54-64. As discussed above, Robert teaches that a variety of implementation options are available for accessing CA protected content on DRM devices. Robert, 8:56-11:59. For example, Robert teaches that access controlled data transmitted to a destination device includes the control words for decrypting content protected by DRM. Robert, 9:53-10:4. By providing the control words, which are obtained by decrypting received ECMs, the destination device can use a DRM license to decrypt CA-protected content. Robert, 4:27-33, 6:31-59, 9:66-10:4. A POSA would have therefore been motivated 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**. Furthermore, a **DSCT 110** configured to operate this way in view of Robert's

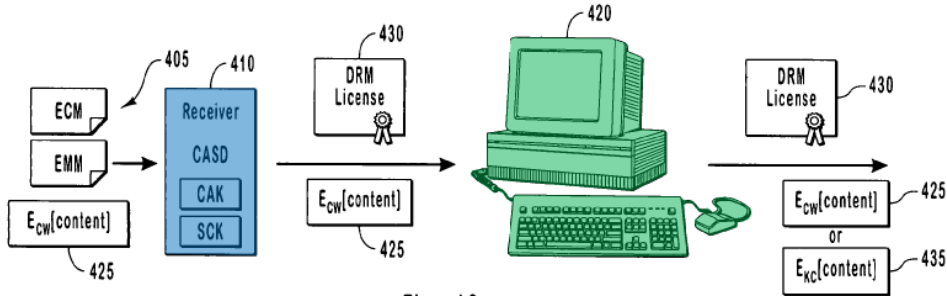
teachings would not be required to decrypt or descramble a service instance before transmitting it to **client-receiver 122**, thereby saving system time and resources. *See also* Russ, 19:50-59 (deciding whether to descramble). Wasilewski, ¶126.

Furthermore, the implementations above would have been, at least, the application of known techniques (*e.g.*, Robert's teachings of transmitting decrypted ECM information, including control words, to destination devices) 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). *See* MPEP §2143 (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421 (2007)).

A POSA would have had a reasonable expectation of success implementing Russ's system by including decrypted ECM information, including control words, as access controlled data. Indeed, both Russ and Robert explain that content protection protocols and encryption schemes are well-known processes. Russ, 17:7-14; Robert, 5:10-11. Robert further explains that variations in the timing and execution of processes (*i.e.*, by different devices) are obvious to POSAs. Robert, 6:52-57. The interpretation and communication of control words of known content protection schemes, on known computing devices, requires only data processing techniques well within the skill of a POSA. Wasilewski, ¶127.

3. Claim Charts (7, 18)

'304	Russ (EX1005) + Robert (EX1006)
7. The medium in claim 5, wherein the content comprises a decrypted version of an entitlement control message.	Robert discloses that the content comprises a decrypted version of an entitlement control message (<i>e.g.</i>, a receiver receiving a control word in an ECM in a controlled access system decrypts the ECM, analyzes the ECM, and transmits ECM contents including the control word to the destination device, now protected via DRM). Wasilewski, ¶¶128-133. In addition to Russ’s disclosure that client-receiver 122 decrypts a service instance with a control word (<i>see</i> Russ, 26:16-28, 26:54-67), Robert teaches including CA control words used by a client device to consume content (<i>i.e.</i>, Russ’s client-receiver 122 and Robert’s destination device 420) in a DRM license sent to the device. 9:66-10:4. For example, a receiver 410 receiving an ECM with control words transcribes the control words into a DRM license such that the destination device 420 can decrypt the CA-protected content with the control words. Robert, 6:31-69, 9:53-10:4. As Robert describes that this is alternative to providing the service keys used for encrypting the control words, a POSA would have recognized that the receiver 410 decrypts the ECM to retrieve the control words—and not leave the control words in an encrypted version of the ECM—for transmission to the destination device 420. A POSA would have been motivated to implement Russ by transmitting a decrypted version of the ECM, including control words, to client-receiver 122 as access controlled data, as taught by Robert, as discussed in §VII.C.2 above. Wasilewski, ¶¶129-132. <i>E.g.</i>, Robert discloses: 6:31-59 (“As will be recognized, there are many ways in which the transcription of the content protection information from conditional access to a digital rights management system can be achieved. <u>For example, as shown in FIG. 3 in the side-by-side comparison of the CA packaging scheme with the DRM packaging system, the multitude of CWs used to encrypt content 310 in accordance with the CA method could be included and transcribed into license 350, thereby allowing license 350</u>

'304	Russ (EX1005) + Robert (EX1006)
	to be used to decrypt the encoded conditional access content. Alternatively, or in addition, the license may include the service keys used to encrypt the CWs, thereby having an additional layer of protection within the license 350 when transcribing to the DRM system.”) - Fig. 4C (showing receiver 410 receiving CA content (ECM and EMM 405, CA-encrypted content 425), translating the information, and transmitting DRM license 430, including a list of CWs, to destination device 420 for consuming the content)  The diagram illustrates the process of receiving and transmitting content and license information. On the left, a 'Receiver' (410) is shown as a blue box containing 'CASD', 'CAK', and 'SCK'. It receives three inputs: 'ECM' (405), 'EMM' (405), and 'E_{CW}[content]' (425). The receiver outputs a 'DRM License' (430) and 'E_{CW}[content]' (425) to a destination device (420), which is depicted as a green computer. The destination device then outputs a 'DRM License' (430) and either 'E_{CW}[content]' (425) or 'E_{KC}[content]' (435). Fig. 4C 9:53-10:4 (“FIG. 4C illustrates another example implementation for producing a content license 430 used to consume content 425, 435 in accordance with usage rights defined by CPI in a CA system. <u>Again, receiver 410, which is a CASD, e.g., CAK, SCK, etc., receives CAM 405 and CA-protected content 425. In this implementation, however, receiver 410 is capable of producing or generating DRM license 430 and sending such license 430 to the destination DRM device 420. In this particular implementation, receiver 410 also sends CA-protected content 425 “as is” to the destination device 420. The destination device 420 may then decrypt the protected content 425, re-encrypt the content in accordance with DRM schemes to produce protected content 435 and update the DRM license 430 with the appropriate content protection key(s). Alternatively, receiver 410 could have included the appropriate keys (e.g., a list of CWs) in DRM license 430 when sent to destination device 420, such that destination device 420 can use the DRM license 430 to decrypt the CA-protected content 425 in it's original</u>

'304	Russ (EX1005) + Robert (EX1006)
	<u>form.</u>”) See also: • 6:43-59 (“any combination and number of possible mappings between the CA and DRM syntax is possible”)
18. The method in claim 16, wherein the content comprises a decrypted version of an entitlement control message.	See claim 7.

VIII. NO BASIS FOR DISCRETIONARY DENIAL

A. *Fintiv*

Under the Director’s Interim Procedure for Discretionary Denials, the Board will not deny institution based on *Fintiv*³ if there is compelling evidence of unpatentability, which this Petition provides, thereby concluding the *Fintiv* analysis. *Nokia of Am. Corp. v. TQ Delta, LLC*, IPR2022-00471, Paper 11 at 19-21 (Aug. 18, 2022). Regardless, the *Fintiv* factors also weigh against discretionary denial.

³ *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential).

1: Petitioner will seek a stay pending resolution of this IPR.

2: D. Del.’s median time to trial is approximately 38 months (EX1016, 14), approximately 1 year after a final written decision would be expected in this IPR.

3: To date, the court has not issued any substantive orders regarding the ’304.

4: After the final written decision, the same grounds and arguments could not be presented in the litigation.

5: The litigation and PTAB parties are the same.

6: Petitioner is highly likely to prevail with respect to the Claims as shown herein.

B. *Advanced Bionics*

The Examiner during prosecution of the ’304 did not consider Russ or art with substantially the same disclosures (or the same or substantially the same arguments) as those herein. Although Applicant cited Robert in an IDS (*see* ’304FH, 85), the Examiner never discussed or applied Robert in any rejection and did not consider Robert in combination with Russ.

Even if the art and arguments were substantially the same, the Examiner erred in a manner material to the patentability of the Claims. Where the “Examiner did not expressly consider” Russ and Robert, it is difficult, if not impossible, to explain “why the Examiner allowed the claims” or “how the Examiner might have

considered the arguments presented in the Petition.” *Bowtech, Inc. v. MCP IP, LLC*, IPR2019-00379, Paper 14 at 20 (July 3, 2019) (declining to exercise §325(d) discretion). And, to the extent the Examiner considered references that purportedly teach the substitution of one security domain for another, the Examiner erred in failing to reject the Claims over a combination of any of those references and art teaching content protection schemes.

Discretionary denial under §325(d) is not warranted.

IX. CONCLUSION

The Board should institute IPR and cancel claims 5-8 and 16-19 of the ’304.

Dated: June 14, 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 June 14, 2024, I will cause a copy of the foregoing document, including any exhibits or appendices filed therewith, to be served via Overnight FedEx at the following correspondence address of record for the patent:

Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

Courtesy copies of the same documents were also served at the following email addresses of record for Patent Owner's litigation counsel:

M. Elizabeth Day	eday@bdiplaw.com
Marc Belloli	mbelloli@bdiplaw.com
Jerry D. Tice II	jtice@bdiplaw.com
Aaron R. Hand	ahand@bidplaw.com
Hillary Bunsow	hbunsow@bdiplaw.com

Date: June 14, 2024

/MacAulay Rush /
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing IPR petition contains 11,181 words excluding a table of contents, a table of authorities, Mandatory Notices under § 42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: June 14, 2024

/MacAulay Rush /
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.