

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASUSTEK COMPUTER INC.,
Petitioner

v.

VIDEOLABS, INC.,
Patent Owner

Inter Partes Review Case No. IPR2024-00304
U.S. Patent No. 8,291,236

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,291,236**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8(A)(1)	6
A.	REAL PARTY-IN-INTEREST	6
B.	RELATED MATTERS	6
C.	LEAD AND BACK-UP COUNSEL	7
D.	37 C.F.R. § 42.8(B)(4) – SERVICE INFORMATION	7
III.	REQUIREMENTS FOR IPR.....	8
A.	GROUND FOR STANDING (37 C.F.R. §42.104(A))	8
B.	IDENTIFICATION OF CHALLENGE (37 C.F.R. §42.104(B)).....	8
1.	<i>Specific Art on Which the Challenge is Based</i>	8
2.	<i>Statutory Grounds on Which the Challenge is Based</i>	8
IV.	BACKGROUND	9
A.	'236 PATENT	9
B.	PROSECUTION HISTORY OF THE '236.....	12
V.	LEVEL OF ORDINARY SKILL IN THE ART	13
VI.	CLAIM INTERPRETATION	13
A.	“ACCESS CONTROLLED DATA THAT IS IN AN ACCESS CONTROLLED FORMAT AND THAT IS AT LEAST PARTIALLY DERIVED FROM THE SECURITY MESSAGES”	14
VII.	GROUND OF UNPATENTABILITY	16
A.	GROUND 1: CLAIMS 32-34, 38-39, 66-68, 72-73, 130-131, AND 134-135 ARE ANTICIPATED BY RUSS.....	16
1.	<i>Overview: Russ</i>	16
2.	<i>Claim Charts (130-131, 134-135)</i>	20
3.	<i>Claim Charts (32-34, 38-39, 66-68, 72-73)</i>	63
B.	GROUND 2: CLAIMS 32-34, 38-39, 66-68, 72-73, 130-131, AND 134-135 ARE OBVIOUS OVER RUSS	84
C.	GROUND 3: CLAIMS 35-36, 69-70, AND 132-133 ARE OBVIOUS OVER RUSS IN VIEW OF ROBERT	85
1.	<i>Overview: Robert</i>	85
2.	<i>Motivation: Russ in view of Robert</i>	86
3.	<i>Claim Charts (132-133)</i>	91
4.	<i>Claim Charts (35-36, 69-70)</i>	97

D.	GROUND 4: CLAIMS 40-41, 43, 74-75, 77, AND 136-137 ARE OBVIOUS OVER RUSS IN VIEW OF ESKICIOGLU	100
1.	<i>Overview: Eskicioglu</i>	100
2.	<i>Motivation: Russ in view of Eskicioglu</i>	102
3.	<i>Claim Charts (136-137)</i>	105
4.	<i>Claim Charts (40-41, 43, 74-75, 77)</i>	111
VIII.	NO BASIS FOR DISCRETIONARY DENIAL	119
A.	FINTIV	119
IX.	CONCLUSION.....	119

TABLE OF AUTHORITIES

Cases:

<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020).....	95
<i>In re Arkley</i> , 455 F.2d 586 (C.C.P.A. 1972)	19
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	74, 86
<i>Net MoneyIN, Inc. v VeriSign, Inc.</i> , 545 F.3d 1359 (Fed. Cir. 2008).....	19
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013, 1017 (Fed. Cir. 2017).....	13
<i>Nokia of Am. Corp. v. TQ Delta, LLC</i> , IPR2022-00471, Paper 11 (PTAB Aug. 18, 2022)	95
<i>Sotera Wireless, Inc. v. Masimo Corporation</i> , IPR2020-1019, Paper 12 at 17-19 (P.T.A.B. Dec. 1, 202) (precedential, designated Dec. 17, 2020).....	119

TABLE OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 8,291,236 (“236”)
1002	File History of U.S. Patent Application No. 11/007,116 (“236FH”)
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	U.S. Patent No. 8,332,657 (“Eskicioglu”)
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	RESERVED
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	RESERVED
1016	Federal Judicial Caseload Statistics (Dec. 31, 2023)
1017	RESERVED

I. INTRODUCTION

Petitioner ASUSTeK Computer Inc. (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 32-36, 38-41, 43, 66-70, 72-75, 77, and 130-137 (“Claims”) of U.S. Patent No. 8,291,236 (EX1001; “’236”) 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 a variety of content protection schemes. ’236, 1:5-10; *see also* EX1006 (“Robert”), 1:21-25. Two well-known schemes are conditional access (CA) and digital rights management (DRM). ’236,1:13-2:52; 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. ’236, 1:19-21, 1:25-28, 1:32-34; 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. ’236, 1:41-56; Robert, 4:51-59. Thus, CA systems protect content via several levels of encryption and messages.

In a DRM system, content is encrypted, and rights to the content are obtained separately, for example from a license issuer. '236, 2:31-40; Robert, 4:64- 5:58. Typically a single key is provided to decrypt the content. Robert, 5:52-58.

The '236 is also directed to systems for limiting the access of audiovisual content. '236, 1:5-10. The '236 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.” '236, 2:56-67. Thus a system according to the '236 may include a primary server distributing content to a secondary server that re-distributes the content to secondary clients. '236, 2:61-4:3.

As shown in Fig. 2A below, **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). '236, 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**. '236, 7:33-39. In the secondary security domain, **secondary CA server 255** acts as a control information provider to conditionally allow secondary CA **clients** to access the content. '236, 7:37-43. Thus, “secondary CA clients in the secondary

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

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.” ’236, 7:26-31 (reference numerals omitted).

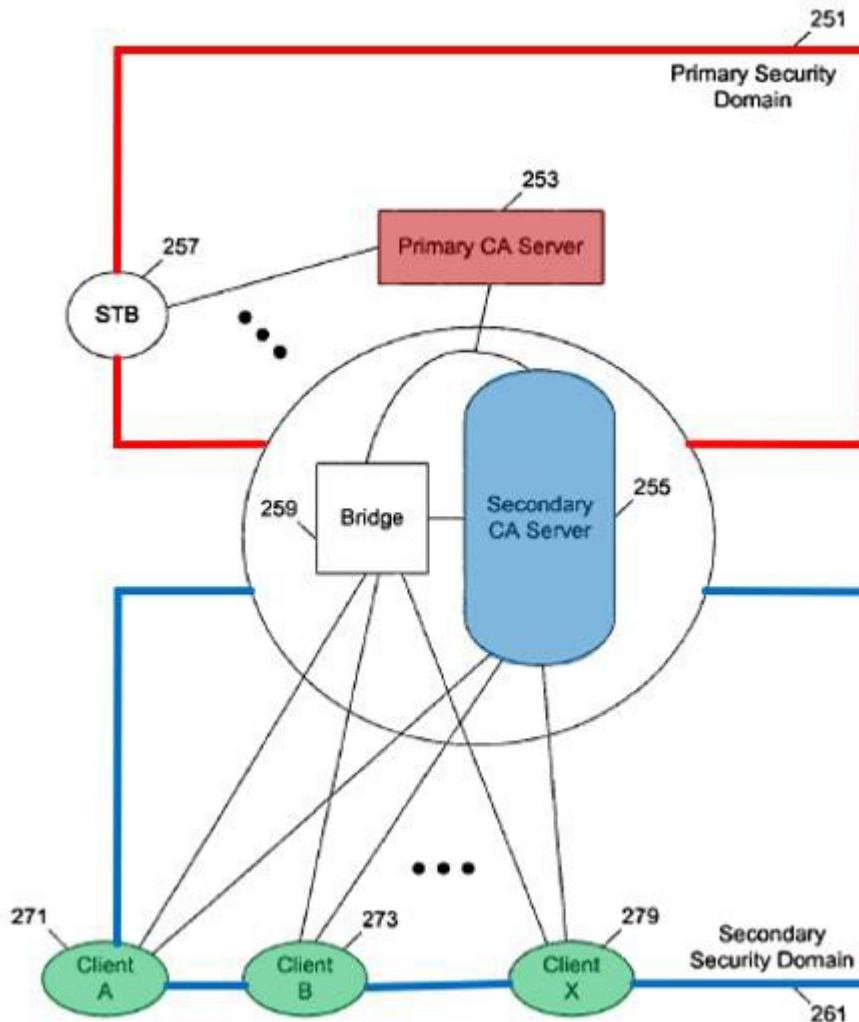
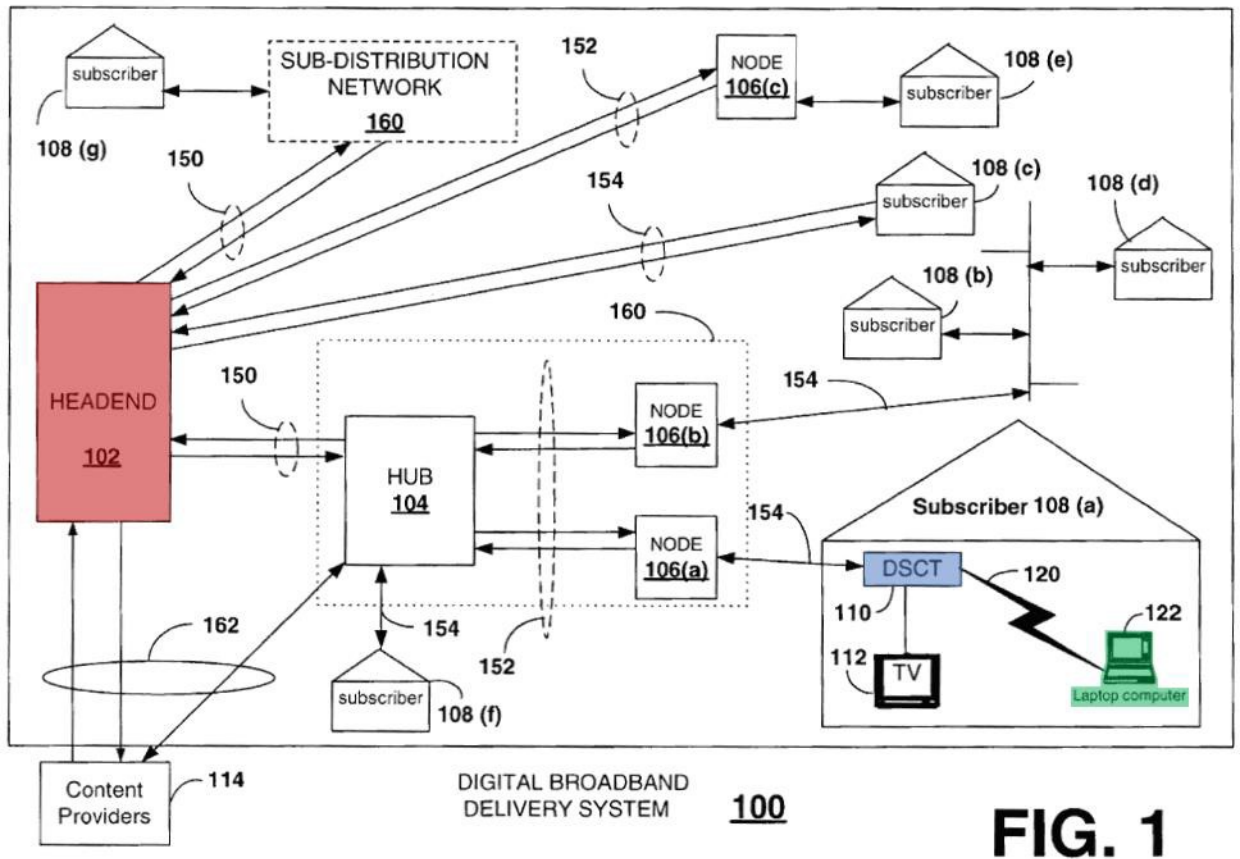


Fig. 2A

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. '236, 2:61-3:16.

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 '236. Russ therefore anticipates at least the independent claims of the '236. Additional features claimed in dependent claims, like the derivation of rights to access controlled data, transmission of specific data including control words, descrambled content, or substitutive ECMs, were also well known, as evidenced by Robert (EX1006) and Eskicioglu (EX1007) discussed below. The USPTO did not consider Russ, alone or in combination with Robert or Eskicioglu, during the '236'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)(1)

A. Real Party-In-Interest

Petitioner identifies ASUSTeK Computer 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 '236 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

The '236 is also subject to the following instituted proceedings before the Board that Petitioner now seeks to join as copycat petitions with an understudy role:

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

Petitioner's copycat petitions:

Title	Patent	IPR No.
<i>ASUSTeK Computer Inc. v. VideoLabs, Inc.</i>	8,291,236	IPR2025-0304
		IPR2025-0305
		IPR2025-0306

C. Lead and Back-Up Counsel

Petitioner provide the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Eric A. Buresh (Reg. No. 50,394) eric.buresh@eriseip.com PTAB@eriseip.com	Christopher R. Schmidt (Reg. No. 63,982) chris.schmidt@eriseip.com PTAB@eriseip.com
<u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	<u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

D. 37 C.F.R. § 42.8(b)(4) – Service Information

Please address all correspondence to the lead and back-up counsel as shown above. Petitioner consents to electronic service by e-mail at the e-mail addresses provided above.

III. REQUIREMENTS FOR IPR

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

Petitioner certifies the '236 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)
Eskicioglu	1007	8,332,657	2002-02-01	2012-12-11	(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	32-34, 38-39, 66-68, 72-73, 130-131, 134-135	Russ
3	§103	35-36, 69-70, 132-133	Russ in view of Robert
4	§103	40-41, 43, 74-75, 77, 136-137	Russ in view of Eskicioglu

IV. BACKGROUND

A. '236 Patent

The '236 discusses methods and apparatuses for bridging two security systems for content delivery in cable television systems, satellite television systems, and the like. '236, 1:5-10, 2:56-59. Such security systems are known and, for example, use “conditional access (CA)” or “digital rights management (DRM)” techniques. '236, 1:13-2:52.

As discussed in §I, 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). '236, 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**. '236, 7:26-31.

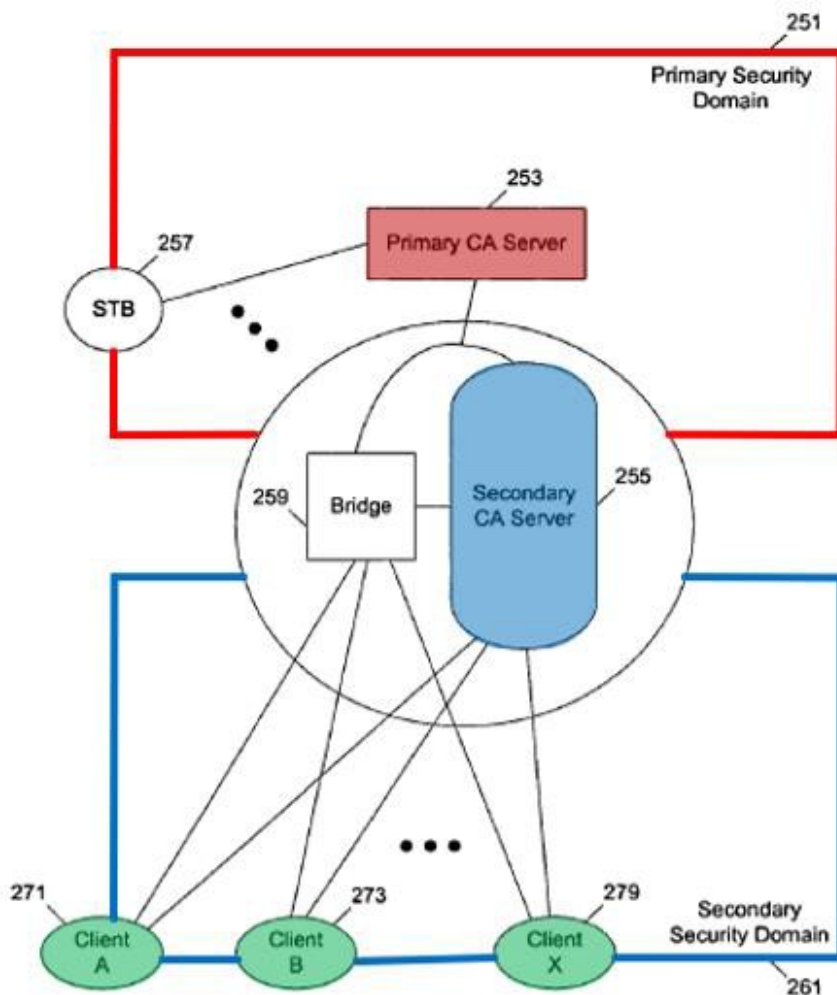


Fig. 2A

And, as discussed, while Fig. 2A shows two CA servers, different embodiments alternatively use DRM techniques or a mix of CA and DRM techniques. '236, 2:61-3:16. Accordingly, bridging in the '236 involves a primary server providing content to an authorized second server, and the second server re-distributing the content to authorized clients.

The '236 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 may be combined along with **storage 605** (*see* '236, 17:16-41, 18:9-18)—receiving broadcast feed 601 from a primary security system. '236, 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. '236, 17:55-61. However, **renderer 607** wanting access to the content is provided with the control word 619 protected by DRM after the **secondary CA server 609** 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. '236, 18:44-54.

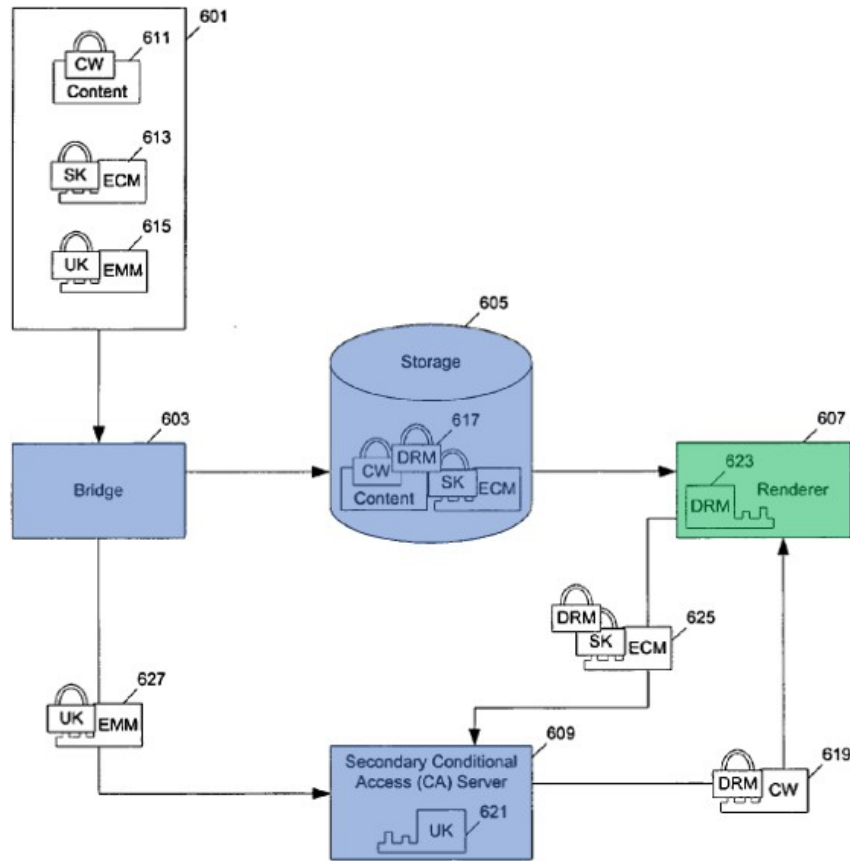


Fig. 11

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

B. Prosecution History of the '236

The '236 issued from U.S. Application No. 11/007,116 (filed 2004-12-07). EX1002 (“’236FH”), 1-129.

During prosecution, the Examiner repeatedly rejected the pending claims as being unpatentable over prior art.’236FH, 296-324, 388-422, 506-541. In an amendment preceding allowance of the claims, the independent claims were amended 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.

The Examiner identified the “wherein” clause as reasons for allowance.’236FH, 624. Wasilewski, ¶¶43-46.

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, ¶¶47-48.

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 (Fed. Cir. 2017).

A. “access controlled data that is in an access controlled format and that is at least partially derived from the security messages”

Claims 32[c], 66[c], and 130[b.ii] recite “access controlled data that is in an access controlled format and that is at least partially derived from the security messages.” This limitation should be interpreted according to its ordinary and customary meaning: “access controlled data that is in an access controlled format” “and [access controlled data that] is at least partially derived from the security messages.” A plain English reading of the claims confirms that the object restricted by “that” is the access controlled data. PO’s attempts to rewrite its claims to shift the second “that” from the object of the first restriction (*i.e.*, to the access controlled format) fails.

In district court, PO asserts infringement of this limitation, stating: “Content is transmitted to the connected TV... over the HDMI interface as HDCP encrypted content in accordance with the requirements of the HDCP enforcement security messages specified by the primary security system platform,” and shows the following figure:

OPL	Compressed Digital Video	Uncompressed Digital Video		Analog TV
	Any	HDMI, DVI, DisplayPort, MHL		Component, Composite
0-100	Block	Passes content		Passes content
101-150				Passes content when CGMS-A CopyNever is engaged or if CGMS-A can't be engaged.
151-200				Passes content when CGMS-A CopyNever is engaged.
201-250		Attempts to engage HDCP, but passes content regardless of result.		Does NOT pass content
251-270		SWDRM: Attempts to engage HDCP. If HDCP fails to engage, the PC will constrain the effective resolution to 520,000 pixels per frame and pass the content.	HWDRM: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked.	
271-300		When HDCP type restriction is NOT defined: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked. When HDCP type restriction IS defined: Passes content with HDCP 2.2 and content stream type set to 1. If HDCP fails to engage or content stream type can't be set to 1, playback to HDMI/DVI ports is blocked.		
> 300		Does NOT pass content		

EX1008, 17-18 (annotation in original).

Thus, PO appears to be asserting a different interpretation with “access controlled data that is in an access controlled format ~~and~~ that is at least partially derived from the security messages”—reading out “and” from the claims.

To the extent this is PO's position, Petitioner disagrees because it improperly reads out a word from the claims. Petitioner is not aware of any embodiment within the '236 where the "access controlled format is... derived from the security messages." Wasilewski, ¶¶49-51.

Nevertheless, construction of this term is not necessary at this time, as the prior art discloses this limitation under either interpretation, as discussed in §VII.A.2-VII.A.3.

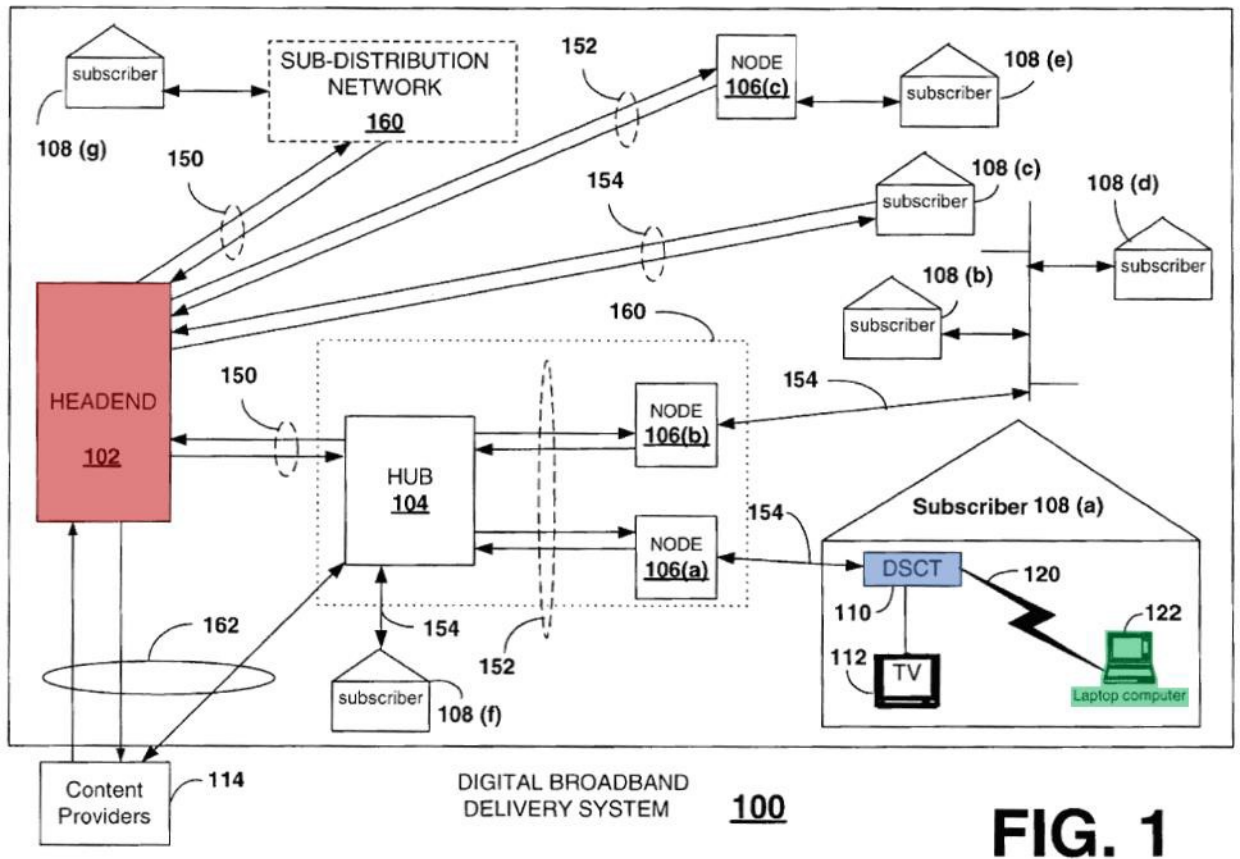
VII. GROUNDS OF UNPATENTABILITY

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 '236. Wasilewski, ¶¶1-244. The prior art renders the Claims unpatentable for reasons discussed below.

A. Ground 1: Claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 are Anticipated by Russ

1. Overview: Russ

Russ describes an "Apparatus for Entitling Remote Client Devices," in which a device receives service instances and entitlement information from a headend of a network and re-transmits service instances to client-receivers with dynamically determined encryption schemes. EX1005 ("Russ"), Title, Abstract, 2:55-3:22. An exemplary distribution system is shown in Fig. 1:



In digital broadband delivery system (DBDS) 100, **headend 102** communicates with content providers 114 to obtain services such as broadcasts or video-on-demand, 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** (e.g., computers, televisions, or set-top terminals). Russ, 5:52-6:32, 6:51-61, 8:38-9:25, 14:1-3. Wasilewski, ¶¶53-54.

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, *e.g.*, 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, then provides 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 authority for **client-receiver 122** and grants/deletes **client-receiver 122's** entitlements to service instances based on information 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, ¶¶55-58.

The specific protection with which **DSCT 110** and **client-receiver 122** communicate is determined dynamically when **client-receiver 122** joins **DSCT 110's** network and provides its device and hardware information. Russ, 3:17-20, 16:64-17:60, 20:12-20. Thus, depending on **client-receiver 122's** classification, *e.g.*, **DSCT 110** communicates with **client-receiver 122** using different protocol and encryption schemes like SSL or Digital Transmission Content Protection (DTCP) protocols. Russ, 17:4-14. Wasilewski, ¶56.

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

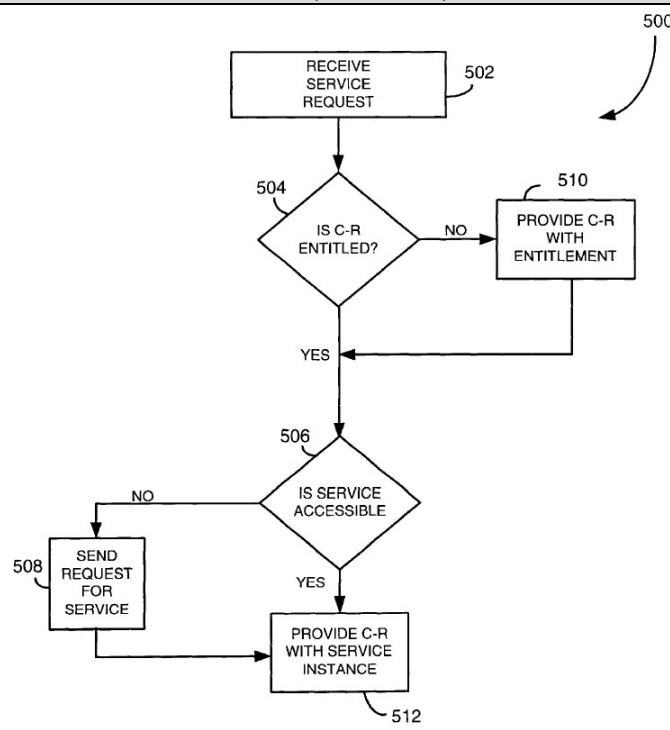
wholly separately negotiated encryption scheme (e.g., DTCP used between **DSCT 110** and **client-receiver 122** but not between **headend 102** and **DSCT 110**), Russ discloses the conditional access server, method to process conditional access protection, and non-transitory machine readable medium as arranged in the claims of the '236. 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 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 of the '236. Wasilewski, ¶¶68-186.

2. *Claim Charts (130-131, 134-135)*

'236	Russ(EX1005)
130[pre²]. A conditional access server, comprising:	Russ discloses a conditional access server (e.g., DSCT 110). Russ discloses a digital broadband distribution system (DBDS) 100 including a digital subscriber communication terminal (DSCT) 110 that is a conditional access server. Russ, 5:35-39. DSCT 110 is a conditional access server because it communicates with, and serves service instances to, client-receiver 122 , and “has the authority and capacity to grant and delete entitlements to the client-receiver 122.” Russ, 8:49-51, 17:61-18:51. Wasilewski, ¶¶68-73. <i>E.g.,</i> Regarding a system including DSCT 110 and client-receiver 122 : Fig. 1:

² Regardless of whether the preambles (130[pre], 32[pre], 66[pre]) are limiting, the prior discloses it.

'236	Russ(EX1005)
	<div data-bbox="492 254 1433 898"> </div> <p style="text-align: right;">FIG. 1</p> <ul style="list-style-type: none"> 5:35-39 (“<u>[D]igital broadband distribution system (DBDS) 100 includes...a headend 102..., digital subscriber communication terminals (DSCTs) 110.</u>”) 8:49-51 (“<u>[C]lient-receiver 122 is in two-way communication with the DSCT 110 and receives information and service instances therefrom.</u>”) <p>Regarding DSCT 110 being a conditional access server to client-receiver 122:</p> <ul style="list-style-type: none"> Fig. 5:

'236	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] 508 --> 512[PROVIDE C-R WITH SERVICE INSTANCE 512] 506 -- YES --> 512 </pre> <p>FIG. 5</p> <ul style="list-style-type: none"> 17:61-18:66 (“Referring to FIG. 5.... In step 502, <u>the DSCT 110 receives a request from the client-receiver 122 for a service instance....</u> <p>In step 504, the secure element 312... determines whether or not the client-receiver 122 is entitled to the requested service instance.</p> <p>In step 510, the client-receiver 122 is provided with the entitlement.... Typically, the secure element 314 generates an EMM, which includes the entitlement, and sends the entitlement to the client-receiver 122.... 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></p> <p><u>The secure element 314 of the DSCT 110 then processes the EMM and provides the entitlement to the client-</u></p>

'236	Russ(EX1005)
	<p><u>receiver 122. In step 512, the selected service instance is provided to the client-receiver 122.”)</u></p> <p><i>See also:</i></p> <ul style="list-style-type: none"> • 3:11-22, 4:21-39, 8:38-9:7, 19:7-42, 24:3-7, 24:37-38
<p>130[a]. one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain;</p>	<p>Russ discloses one or more communication interfaces (<i>e.g.</i>, input-port 302, tuner 304, transceiver 308) to receive security messages of a primary security system (<i>e.g.</i>, to receive entitlement management messages (EMMs) of/from headend 102; EMMs include entitlement and key information) in a first security domain (<i>e.g.</i>, headend 102 implements conditional access authority (CAA) logic to control access to service instances for a plurality of DSCTs 110; headend 102 and DSCT 110 exchange public keys to establish and conduct secure communications with each other). Wasilewski, ¶¶74-79.</p> <p>Russ discloses that DSCT 110 (for example as shown at subscriber location 108(a) in Fig. 1 below) may be one of many DSCTs whose access to DBDS 100 is controlled by headend 102 through entitlements. Russ, 8:4-22. DSCT 110 registers with headend 102 and securely communicates with headend 102 after exchanging public key information. 6:62-7:6, 7:56-8:22, 10:48-65. Accordingly, headend 102 represents a primary security system in a first security domain in which DSCT 110 is a member. Wasilewski, ¶¶77-78.</p> <p>Russ further discloses that headend 102 transmits EMMs to DSCT 110 to provide entitlement information regarding service instances. Russ, 8:4-37, 10:48-65; <i>see</i> '236 claim 131 (security messages include EMMs). DSCT 110 receives such communications on input-port 302 and transceiver 308. Russ, 13:53-56, 14:36-42. Wasilewski, ¶¶75-76.</p> <p><i>E.g.,</i></p> <p>Regarding a primary security system, including headend 102, in a first security domain with DSCT 110:</p> <ul style="list-style-type: none"> • Fig. 1

'236	Russ(EX1005)
	<div data-bbox="493 252 1435 898"> <p style="text-align: center;">DIGITAL BROADBAND DELIVERY SYSTEM 100</p> </div> <p style="text-align: right;">FIG. 1</p> <ul style="list-style-type: none"> 6:62-7:6 (“Secure communication between the headend 102 and the DSCTs 110... using... (RSA) public key encryption.... <u>The headend 102 and the DSCT 110 can securely communicate after they have exchanged public keys.</u>”) 7:56-58 (“Before the <u>DSCT 110 receives and accesses service instances from the headend 102</u>, the <u>DSCT 110 is registered with the headend 102 and entitled to the service instances.</u>”) 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.... The content of a secure message may be encrypted...</u>”) 10:48-65 (“<u>The CAA 234 is used by the access controlling authority to enable DSCTs 110 to receive entitlements for service instances.... To create an EMM, the CAA 234 includes a message content and an authentication token in</u>

'236	Russ(EX1005)
	<p><u>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.... 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.”)</u></p> <p>Regarding security messages, <i>e.g.</i>, EMMs of headend 102:</p> <ul style="list-style-type: none">• 8:25-34 (“The DSCT 110 authenticates the EMM using the trusted public key of the conditional access authority and acts upon the EMM.... <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> <p>Regarding DSCT 110 receiving EMMs:</p> <ul style="list-style-type: none">• Fig. 3

'236	Russ(EX1005)
	<p style="text-align: center;">FIG. 3</p> <ul style="list-style-type: none"> 13:53-56 (“<u>DSCT 110 is adapted to receive in-band and out-of-band communication at input-port 302....</u>”) 14:36-42 (“<u>[T]ransceiver 308 receives out-of-band communication 258 from input port 302. The out-of-band communication data includes... secure messages such as EMMs. EMMs are sent to the secure element 314 for processing....</u>”) <p>See also:</p> <ul style="list-style-type: none"> 7:7-20, 7:56-8:3, 10:39-56, 11:37-61
130[b.i].	Russ discloses a processor coupled to the one or more

'236	Russ(EX1005)
a processor coupled to the one or more communication interfaces, the processor to process the security messages, and	<p>communication interfaces (<i>e.g.</i>, secure element 314 includes processor 702 and is coupled to input-port 302 and transceiver 308) to process the security messages (<i>e.g.</i>, to process EMMs).</p> <p>Russ discloses that DSCT 110 includes secure element 314, which is a processor including processor 702 (which itself includes an authorization/entitlement management module (AEMM) 720)) and memory 704. Russ, Figs. 3 and 7, 20:25-26, 21:11-21. EMMs received at input-port 302 and transceiver 308 are sent to secure element 314 for processing by the AEMM. 14:36-42, 18:60-19:6, 21:11-21. Wasilewski, ¶¶80-83.</p> <p><i>E.g.</i>,</p> <p>Regarding DSCT 110 including a processor coupled to communication interface(s):</p> <ul style="list-style-type: none"> • Fig. 3

'236	Russ(EX1005)
------	--------------

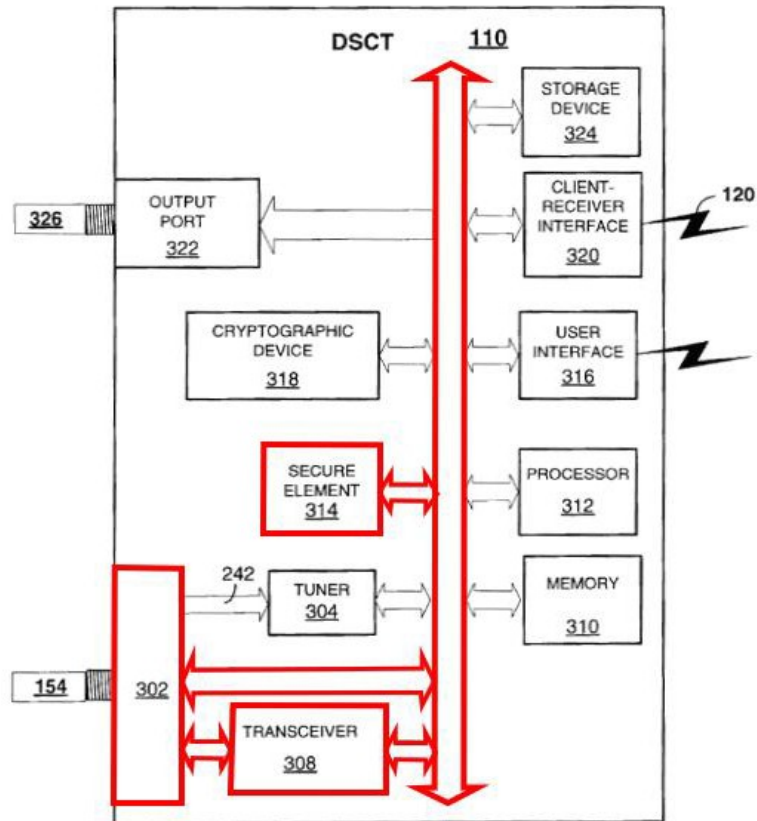


FIG. 3

- Fig. 7

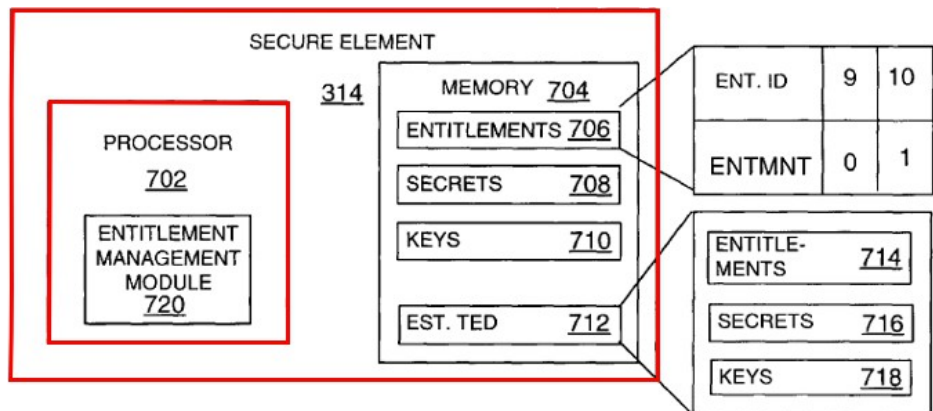


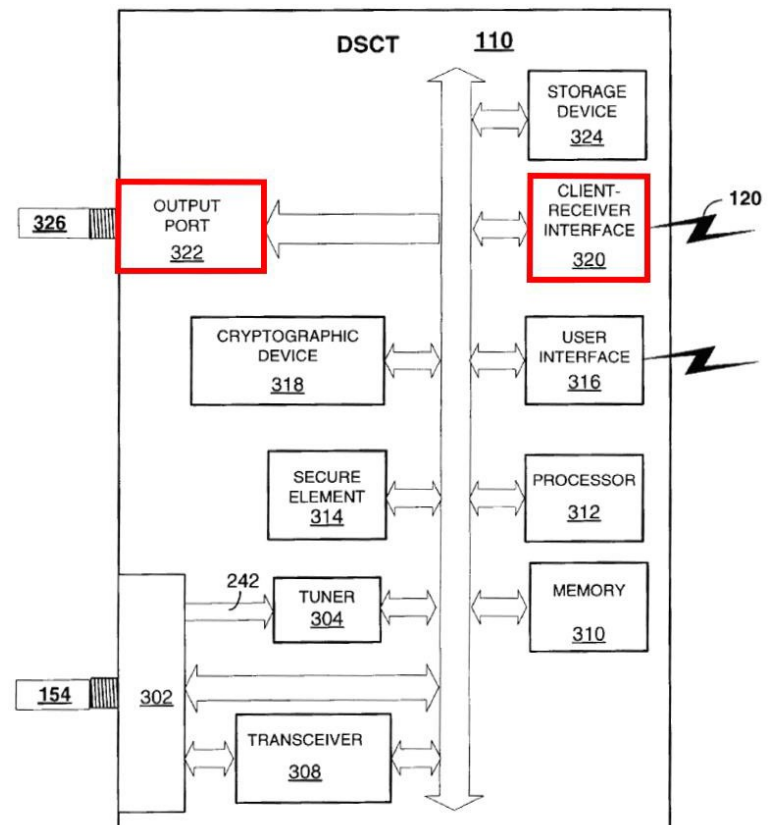
FIG. 7

'236	Russ(EX1005)
	<ul style="list-style-type: none"> 20:25-26 (“<u>[S]ecure element 314 includes a processor 702 and a memory 704.</u>”) <p>Regarding processing EMMs:</p> <ul style="list-style-type: none"> 14:36-42 (<i>see</i> claim 130[a]) 18:62-65 (“<u>The secure element 314 of the DSCT 110 then processes the EMM....</u>”) 21:11-21 (“<u>The processor 702 includes an authorization/entitlement management module (AEMM) 720. The AEMM 720 provides entitlements to the client-receiver 122 for service instances. The AEMM 720 also... generates secure messages for the client-receiver 122.... AEMM 720 receives EMMs for the DSCT 110 from the headend 102..., and the AEMM 720 authenticates them.... AEMM 720 responds to the EMMs and implements them.</u>”) <i>See also</i> 18:60-19:6, 22:40-23:67, 24:25-36.

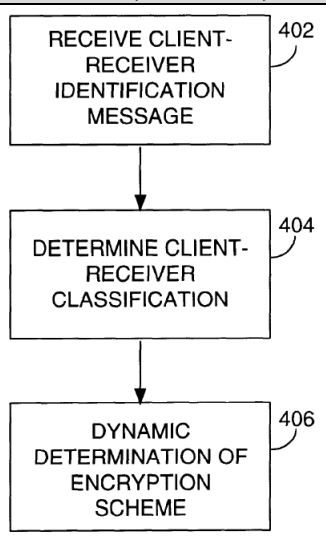
130[b.ii]. the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least	Russ discloses the one or more communication interfaces to transmit, to a secondary conditional access client (<i>e.g.</i> , DSCT 110 further includes an output port 322 and client-receiver interface 320 to communicate with client-receiver 122) through a network connection (<i>e.g.</i> , client-receiver 122 joins DSCT 110's network and communicates via communication link 120) in a second security domain (<i>e.g.</i> , content transmitted from DSCT 110 to client-receiver 122 is encrypted for privacy; the encryption scheme is dynamically determined between the DSCT 110 and client-receiver 122; shared secrets between DSCT 110 and client-receiver 122 are used to encrypt/decrypt the content and thus protect the content from unauthorized access), access controlled data that is in an access controlled format (<i>e.g.</i> , DSCT 110 transmits EMMs and service instances to client-receiver 122 using the dynamically determined encryption scheme) and that is at least partially derived from the security messages (<i>e.g.</i> , DSCT 110 is entitled to a service instance via EMM; DSCT 110 receives entitlements in the EMM, then provides entitlements to client-receiver 122). Wasilewski, ¶¶84-92.
--	---

'236	Russ(EX1005)
partially derived from the security messages,	<p>Russ discloses that DSCT 110 includes an output port 322 and client-receiver interface 320 for wired and/or wireless communications to devices such as televisions and client-receiver 122. Russ, 13:53-65. For example, client-receiver 122 joins a local network managed by DSCT 110, and they communicate over communication link 120 using an Ethernet connection or 802.11a standard. Russ, Fig. 1, 8:38-48, 9:8-20. Wasilewski, ¶85.</p> <p>As discussed with respect to claim 130[pre], client-receiver 122 is a conditional access client to DSCT 110, which serves service instances to client-receiver 122 (and to other devices and client-receivers at the subscriber location) and grants and deletes entitlements to client-receiver 122. Communications between DSCT 110 and client-receiver 122 are conducted via a dynamically determined encryption scheme that is negotiated when client-receiver 122 joins DSCT 110's network. Russ, 16:64-17:60, 20:14-24. Furthermore, client-receiver 122 and DSCT 110 share secrets specifically used to encrypt service instances provided to client-receiver 122. Russ, 20:25-53. Accordingly, because DSCT 110 and client-receiver 122 communicate within their own network, with an encryption scheme that is specifically used between DSCT 110 and client-receiver 122 and involving keys shared between DSCT 110 and client-receiver 122, communications between DSCT 110 and client-receiver 122 are conducted in a second security domain in an access controlled format. Wasilewski, ¶¶86-89.</p> <p>Examples of access controlled data transmitted between DSCT 110 and client-receiver 122 include encrypted entitlement data and services instances in the format negotiated between DSCT 110 and client-receiver 122 as discussed above, decrypted and encrypted by cryptographic device 318. Russ, 15:46-52, 16:64-17:60, 20:14-24, 21:11-65. Entitlements transmitted to client-receiver 122 are, for example, based on the EMMs received at DSCT 110 and are thus at least partially derived from the security messages. Russ, 18:52-65. Furthermore, DSCT 110 is entitled to service instances by headend 102 via EMMs, and only when DSCT 110 is entitled to a service instance does it decrypt the service instance and re-encrypt it for transmission to</p>

'236	Russ(EX1005)
	<p>client-receiver 122. Russ, 8:8-34, 15:46-52. Therefore, service instances are also partially derived from the security messages. Wasilewski, ¶88.</p> <p><i>E.g.,</i></p> <p>Regarding communication interface(s) transmitting information to client-receiver 122 through a network connection:</p> <ul style="list-style-type: none">• 8:38-48 (“<u>DSCT 110 is preferably in communication with client-receiver 122 via communication link 120.... the communication link 120 is wireless such as... [IEEE] 802.11a, 802.11b, 802.11g... In alternative embodiments, the DSCT 110 is in communication... via... Ethernet....</u>”)• 9:9-12 (“<u>When... client-receiver 122 is brought into the local network, the client-receiver 122 discovers the network and communicates with the DSCT 110.</u>”)• Fig. 3

'236	Russ(EX1005)
	 <p>The diagram shows a central vertical bus labeled 'DSCT 110'. On the left side, there is an 'OUTPUT PORT 322' (highlighted with a red box) connected to a cable labeled '326'. Below it is a 'CRYPTOGRAPHIC DEVICE 318', then a 'SECURE ELEMENT 314'. At the bottom left is a block labeled '302' connected to a cable labeled '154'. On the right side, there is a 'CLIENT-RECEIVER INTERFACE 320' (highlighted with a red box) connected to a wireless link labeled '120'. Below it is a 'USER INTERFACE 316' connected to another wireless link. Further down are a 'PROCESSOR 312' and 'MEMORY 310'. At the bottom right is a 'TUNER 304' connected to a cable labeled '242'. At the very bottom right is a 'TRANSCEIVER 308'. All components are connected to the central DSCT 110 bus via bidirectional arrows.</p>
	<p>FIG. 3</p> <ul style="list-style-type: none"> 13:53-65 (“DSCT 110 is adapted to... <u>output signals via output-port 322 and client-receiver interface 320....</u> [C]lient-receiver interface 320 includes a transceiver for a <u>wireless communication link 120 between the DSCT 110 and a client-receiver 122.</u> In an alternative embodiment, the <u>client-receiver interface 320 includes a transceiver for a wired communication link...</u>”) <p>Regarding DSCT 110 and client-receiver 122 being in a second security domain and communicating information in an access controlled format:</p> <ul style="list-style-type: none"> Fig. 1

'236	Russ(EX1005)
	<div data-bbox="496 260 1435 898"> </div> <p style="text-align: right;">FIG. 1</p> <ul style="list-style-type: none"> 16:64-17:14 (“The memory 310 includes logic for <u>dynamic encryption scheme determination</u>. Generally, the <u>content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication</u>. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is <u>determined by considering factors such as the device type of the client-receiver 122 and the communication medium....</u> Non-limiting examples... include... [SSL] protocol, <u>Digital Transmission Content Protection (DTCP)</u>, [CPRM], and [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.</u>”) Fig. 4

'236	Russ(EX1005)
	 <pre> graph TD 402[RECEIVE CLIENT-RECEIVER IDENTIFICATION MESSAGE] --> 404[DETERMINE CLIENT-RECEIVER CLASSIFICATION] 404 --> 406[DYNAMIC DETERMINATION OF ENCRYPTION SCHEME] </pre> <p style="text-align: center;">FIG. 4</p> <ul style="list-style-type: none"> 17:15-34 (“[S]tep 400 are implemented.... In step 402, the DSCT 110 receives a client-receiver identification message from the client-receiver.... include[ing]... hardware information about 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. 6

'236	Russ(EX1005)
	<div data-bbox="600 252 1339 1249"> <pre> graph TD 602[RECEIVE SERVICE INSTANCE] --> 604{IS SERVICE INSTANCE ENCRYPTED?} 604 -- YES --> 606{DECRYPT SERVICE INSTANCE?} 604 -- NO --> 610{ENCRYPT SERVICE INSTANCE?} 606 -- YES --> 608[DECRYPT SERVICE INSTANCE] 606 -- NO --> 614[TRANSMIT SERVICE INSTANCE] 608 --> 610 610 -- YES --> 612[ENCRYPT SERVICE INSTANCE] 610 -- NO --> 614 612 --> 614 </pre> <p>The flowchart, labeled 600, illustrates a process for handling a service instance. It begins with a rectangular box 602 labeled 'RECEIVE SERVICE INSTANCE'. An arrow points down to a diamond-shaped decision box 604 labeled 'IS SERVICE INSTANCE ENCRYPTED?'. From box 604, a 'YES' path leads right to another diamond-shaped decision box 606 labeled 'DECRYPT SERVICE INSTANCE?'. From box 606, a 'YES' path leads left to a rectangular box 608 labeled 'DECRYPT SERVICE INSTANCE', which then points down to a third diamond-shaped decision box 610 labeled 'ENCRYPT SERVICE INSTANCE?'. From box 604, a 'NO' path leads down directly to box 610. From box 610, a 'YES' path leads down to a rectangular box 612 labeled 'ENCRYPT SERVICE INSTANCE', which then points down to a final rectangular box 614 labeled 'TRANSMIT SERVICE INSTANCE'. From box 610, a 'NO' path leads left and then down to box 614. Box 612 also points down to box 614. Boxes 612 and 614 are highlighted with red borders.</p> </div> <p style="text-align: center;">FIG. 6</p> <ul style="list-style-type: none"> 20:14-24 (“<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> [...] <u>In step 614, the client-receiver interface 320 transmits the service instance to the client-receiver 122.</u>”) 20:25-53 (“<u>[S]ecure element 314 includes... memory 704. The memory 704... includes entitlements 706, secrets 708, and keys 710. [...]</u> <u>The secrets 708 are secrets that are shared between the DSCT 110 and the client-receiver 122.... [S]ecrets 708 are</u>

'236	Russ(EX1005)
	<p>used for... 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.”)</p> <p>Regarding transmission of access controlled data to client-receiver 122:</p> <ul style="list-style-type: none">• 18:52-65 (“[S]ecure element 314 generates a secure message requesting entitlement for the selected service instance for the client-receiver 122 and sends the secure message to the entitlement generator 236.... <p><u>The entitlement generator 236 receives the secure message from the DSCT 110 and provides the entitlement for the selected service instance to the DSCT 110 in an EMM. The secure element 314 of the DSCT 110 then processes the EMM and provides the entitlement to the client-receiver 122.”)</u></p> <ul style="list-style-type: none">• Fig. 6

'236

Russ(EX1005)

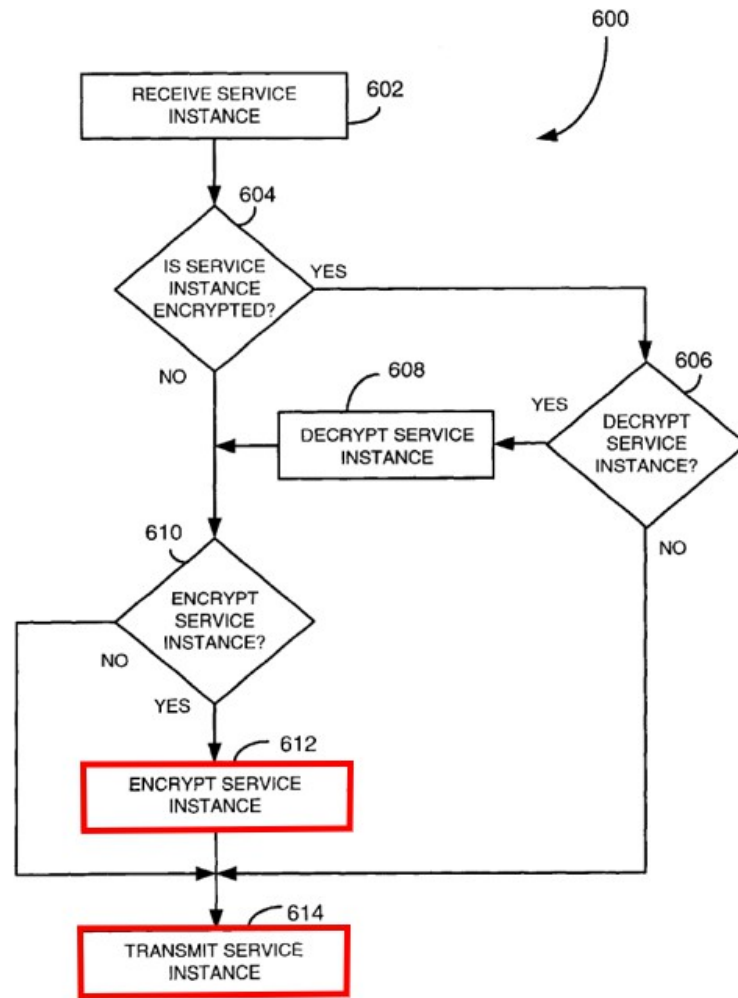


FIG. 6

- 20:14-24 (*see above*)
- 21:11-21 (*see claim 130[b.ii]*)
- 21:22-65 (“Referring now to FIG. 8A, an entitlement management message 800 includes an address field 802, message content 804 and an authentication token 806. EMM 800 is a typical EMM used for securely transmitting information...between the DSCT 110 and the client-receiver 122. The EMM 800 is an exemplary secure message.”)

[...]

'236	Russ(EX1005)
	<p><u>Whether the message content 804 is encrypted depends upon whether or not privacy is desired. ... Whereas, when the message content 804 is related to entitlements, or encryption, or decryption, then the message content 804 will probably be encrypted. Whether the message content 804 is encrypted is a matter of implementation and depends upon the sought after level of security... between the DSCT 110 and the client-receiver 122.”)</u></p> <ul style="list-style-type: none"> • 24:1-24 (“[T]he AEMM 720 includes logic for granting entitlements to the client-receiver 122 for service instances.... <u>If the AEMM 720 determines to grant the entitlement to the client-receiver 122, the AEMM 720 provides the client-receiver 122 with the entitlement via an EMM, and the AEMM 720 changes the entitlements 706 to reflect the newly granted entitlement.... The AEMM 720 can up date the client-receiver’s entitlement map by sending the client-receiver 122 an EMM with new entitlements for the client-receiver 122.”)</u> <p>Regarding deriving access controlled data from security messages:</p> <ul style="list-style-type: none"> • 8:8-22 (<i>see</i> claim 130[a]) • 8:25-34 (<i>see</i> claim 130[a]) • 15:46-52 (“<u>When the DSCT 110 is entitled to the selected service instance.... The cryptographic device 318 decrypts the 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> • 18:52-65 (<i>see</i> above) <p>See also:</p> <ul style="list-style-type: none"> • 1:45-2:10, 3:17-20, 8:44-48, 9:8-20, 13:63-14:3, 16:34-42, 17:15-23, 25:43-50 <p>Additionally, to the extent PO argues that the access controlled format must be derived from the security messages (<i>see</i> §VI.A)—Russ discloses the access controlled format partially derived from the security messages (<i>e.g.</i>, headend</p>

'236	Russ(EX1005)
	<p>102 transmits an EMM to DSCT 110 dictating the encryption scheme for communications with client-receiver 122). Wasilewski, ¶91.</p> <ul style="list-style-type: none"> • 25:17-22 (“<u>system controller 232 can... 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>”) • <i>See also</i> 16:31-63, 19:7-27, 25:22-25.
<p>130[c.i]. wherein the primary security system authenticates the conditional access server clients of the primary security system through a first authentication process using a first root of trust and</p>	<p>Russ discloses that the primary security system authenticates the conditional access server clients of the first primary security system through a first authentication process using a first root of trust (<i>e.g.</i>, 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). Wasilewski, ¶¶93-96.</p> <p><i>E.g.</i>, “Root of trust” is not explicitly defined in the ’236, 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. Wasilewski, ¶95.</p> <p>Regarding headend 102 authenticating DSCT 110 using a first root of trust:</p> <ul style="list-style-type: none"> • 7:21-39 (“<u>[W]hen 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....</u> 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. <u>Each DSCT 110 in the DBDS 100</u>

'236	Russ(EX1005)
	<p><u>has a unique serial number</u>, and the serial number, which can be the MAC address of the DSCT 110, is used for addressing messages to the DSCT 110. <u>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></p> <ul style="list-style-type: none">• 7:56-58 (<i>see</i> claim 130[a])• 7:58-66 (“<u>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.”)</u> <p>See also:</p> <ul style="list-style-type: none">• 7:40-55, 8:4-11, 10:39-47

130[c.ii]. the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication	Russ discloses that the conditional access server authenticates clients of the conditional access server through a second authentication process (<i>e.g.</i> , DSCT 110 and client-receiver 112 have a server-client relationship using Digital Transmission Content Protection (DTCP) protocols, which includes an authentication process) which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust (<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
--	--

'236	Russ(EX1005)
<p>process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and</p>	<p>claim 130[c.i]).</p> <p>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 130[b.ii]. DSCT 110 and client-receiver 122 may thus follow DTCP protocols. Russ, 16:64-17:14. A POSA would have recognized that DTCP protocols include authentication and key and certificate exchange procedures that ensure communications are protected. EX1010 (US 2002/0025042), [0009] (describing AKE under DTCP); EX1011 (US 2005/0027984), [0053] and [0107] (describing device identification numbers embedded in a device certificate issued by a licensing institution), [0139]-[0143] and Fig. 17 (describing a “DTCP communication sequence” including an AKE prior to transmission of content). 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, ¶¶97-102.</p> <p><i>E.g.,</i></p> <ul style="list-style-type: none"> • 16:64-17:14 (<i>see</i> claim 130[b.ii])”)

130[c.iii]. wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.	Russ discloses that the conditional access server is configured to substitute the first security domain with the second security domain (<i>e.g.</i> , DSCT 110 receives the service instance from headend 102, decrypts the service instance, then encrypts the service instance with an encryption scheme specifically negotiated between DSCT 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 the second root of trust established with DSCT 110, <i>see</i> discussion of claim 130[c.i]). 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, 19:50-20:19. Between headend 102 and DSCT 110 , a
---	---

'236	Russ(EX1005)
------	--------------

	<p>service instance may be encrypted/decrypted by a multi-session key and CA control words (<i>see</i> Russ, 11:37-61, 13:14-34), while the re-encrypted service instance is protected by DTCP encryption between DSCT 110 and client-receiver 122 (see discussion of claim 130[b.ii, c.ii]). DSCT 110 therefore substitutes the first security domain using CA with the second security domain using DTCP. Wasilewski, ¶¶103-108.</p> <p><i>E.g.,</i></p> <p>Regarding the first security domain including headend 102 and DSCT 110:</p> <ul style="list-style-type: none">• 11:37-46 (multi-session key (MSK) used to generate control words, the MSK being transmitted to DSCT 110 in EMMs)• 13:14-34 (“<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. 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> <p><u>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.... Typically, the authentication token is a hash digest of the message content and a secret that is shared with the DSCTs 110, such as the MSK. 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></p> <p>Regarding the second security domain including DSCT 110 and client-receiver 122:</p> <ul style="list-style-type: none">• 16:64-17:14 (<i>see</i> claim 130[b.ii])• 17:15-34 (<i>see</i> claim 130[b.ii]) <p>Regarding DSCT 110 substituting the first security domain for the second security domain:</p>
--	---

'236	Russ(EX1005)
	<ul style="list-style-type: none"> 15:46-52 (<i>see</i> claim 130[b.ii]) Fig. 6 <div data-bbox="600 373 1339 1365"> <pre> graph TD 602[RECEIVE SERVICE INSTANCE] --> 604{IS SERVICE INSTANCE ENCRYPTED?} 604 -- YES --> 606{DECRYPT SERVICE INSTANCE?} 604 -- NO --> 610{ENCRYPT SERVICE INSTANCE?} 606 -- YES --> 608[DECRYPT SERVICE INSTANCE] 606 -- NO --> 614[TRANSMIT SERVICE INSTANCE] 610 -- YES --> 612[ENCRYPT SERVICE INSTANCE] 610 -- NO --> 614 608 --> 614 612 --> 614 </pre> <p>The flowchart, labeled 600, illustrates a process for handling a service instance. It begins with a rectangular box 602 labeled 'RECEIVE SERVICE INSTANCE'. An arrow leads down to a diamond-shaped decision box 604 labeled 'IS SERVICE INSTANCE ENCRYPTED?'. From box 604, a 'YES' path leads right to a second diamond-shaped decision box 606 labeled 'DECRYPT SERVICE INSTANCE?'. From box 606, a 'YES' path leads left to a rectangular box 608 labeled 'DECRYPT SERVICE INSTANCE', which then leads down to a final rectangular box 614 labeled 'TRANSMIT SERVICE INSTANCE'. From box 606, a 'NO' path leads down to box 614. From box 604, a 'NO' path leads down to a third diamond-shaped decision box 610 labeled 'ENCRYPT SERVICE INSTANCE?'. From box 610, a 'YES' path leads down to a rectangular box 612 labeled 'ENCRYPT SERVICE INSTANCE', which then leads down to box 614. From box 610, a 'NO' path leads left and then down to box 614. All three paths (from 608, 612, and the direct path from 610) converge at box 614.</p> </div> <p style="text-align: center;">FIG. 6</p> <ul style="list-style-type: none"> 19:52-20:16 (“[W]hen the processor 312 determines to decrypt the service instance.... <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> In step 610, the processor 312 determines an encryption scheme for the selected service instance.... <u>The cryptographic device 318 encrypts the service instance</u>

'236	Russ(EX1005)
	<p><u>using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122.”)</u></p> <p>See also:</p> <ul style="list-style-type: none"> • 8:49-9:7, 23:47-67
<p>131. The conditional access server of claim 130, wherein the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system.</p>	<p>Russ discloses that the security messages comprise entitlement management messages (e.g., DSCT 110 receives EMMs); and the access controlled data is protected using a digital rights management system (e.g., communications between DSCT 110 and client-receiver 122 are protected by a DTCP scheme—a DRM system). Wasilewski, ¶¶109-112.</p> <p>Russ discloses that DSCT 110 receives security messages including EMMs from headend 102. Russ, 8:4-37, 10:48-65, 25:17-25; <i>see</i> discussions of claims 130[a] and 130[b.ii]. Wasilewski, ¶110.</p> <p>Russ further discloses that the access controlled data transmitted from DSCT 110 to client-receiver 122 are protected by DTCP. Russ, 16:64-17:14; <i>see</i> discussion of claim 130[c.ii]. A POSA would have recognized that DTCP is a form of digital rights management system. <i>See, e.g.,</i> EX1012 (US 2003/0078891), [0041] (“The oldest DRM system is known as CCI. Examples of CCI systems include ... DTCP”); EX1013 (US 2004/0098583), [0014] (“Examples of traditional digital rights management authentication methods include ... DTCP”). Wasilewski, ¶111.</p>
<p>134[pre]. The conditional access server of claim 131, wherein</p>	<p><i>See</i> claim 131.</p>
<p>134[a]. the one or more communication interfaces are to receive an</p>	<p>Russ discloses that the one or more communication interfaces (e.g., input-port 302, tuner 304) are to receive an entitlement control message (e.g., receiving an entitlement control message (ECM) from headend 102) and scrambled content of the primary security system (e.g., receiving an encrypted service instance or program from headend 102).</p>

'236	Russ(EX1005)
entitlement control message and scrambled content of the primary security system; and the conditional access server further comprises:	<p>Wasilewski, ¶¶114-118.</p> <p>Russ discloses that DSCT 110 receives communications, via input-port 302 and tuner 304. Russ, 13:53-56. Wasilewski, ¶115.</p> <p>DSCT 110 receives transport stream 242 from multi-transport stream receiver-transmitter 228 of headend 102. Russ, 13:3-5, 15:1-6. Transport stream 242 includes an ECM. Russ, 13:20-23. Wasilewski, ¶¶116-117.</p> <p>DSCT 110 also receives service instances from headend 102. Russ, 7:56-58. Service instances are encrypted with control words and/or with a Digital Video Broadcasting (DVB) Common Scrambling technique. Russ, 12:47-13:19. Wasilewski, ¶117.</p> <p><i>E.g.,</i></p> <p>Regarding input-port 302 and tuner 304:</p> <ul style="list-style-type: none"> • Fig. 3

'236	Russ(EX1005)
	<div data-bbox="597 260 1334 1066" data-label="Diagram"> </div> <p data-bbox="927 1234 1084 1285" style="text-align: center;">FIG. 3</p> <ul data-bbox="521 1318 1419 1541" style="list-style-type: none"> • 13:53-56 (<i>see</i> claim 130[a]) • 15:1-6 (“<u>tuner 304 receives in-band communication from input-port 302.... Typically, the tuner 304 also includes a demultiplexer for demultiplexing the received transport stream 242.</u>”) <p data-bbox="493 1566 1419 1642">Regarding receiving ECMs and scrambled service instances of headend 102:</p> <ul data-bbox="521 1667 959 1768" style="list-style-type: none"> • 7:56-58 (<i>see</i> claim 130[a]) • Fig. 2

'236	Russ(EX1005)
	<div data-bbox="496 249 1435 863" data-label="Diagram"> </div> <p style="text-align: right;">FIG. 2</p> <ul style="list-style-type: none"> 12:47-13:19 (“<u>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... DES..., [DVB] Common Scrambling or other cryptographic algorithms or techniques.... “Entitled” DSCTs 110 are allowed to use the decryption information to decrypt encrypted content....</u> <p><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></p> <ul style="list-style-type: none"> 13:20-23 (“<u>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> <p>See also:</p>

'236	Russ(EX1005)
	<ul style="list-style-type: none"> 5:52-6:7, 13:3-5
<p>134[b]. a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message;</p>	<p>Russ discloses a descrambler coupled to the processor (<i>e.g.</i>, cryptographic device 318 coupled to secure element 314) to descramble the scrambled content according to the entitlement control message (<i>e.g.</i>, to decrypt the service instance with control words generated from the ECM if DSCT 110 is entitled to the service instance according to the ECM).</p> <p>Russ discloses that DSCT 110 includes cryptographic device 318. Russ, Fig. 3. Cryptographic device 318 decrypts the service instance according to a control word generated by secure element 314 from the ECM, which includes an entitlement specifier used to lookup an array element for determining whether DSCT 110 is entitled to a specific service instance and which includes a counter value for generating a control word to decrypt the service instance when DSCT 110 is entitled to do so. Russ, 13:20-39, 15:46-54, 23:25-46, 23:55-67. Wasilewski, ¶¶119-123.</p> <p><i>E.g.</i>, Regarding cryptographic device 318:</p> <ul style="list-style-type: none"> Fig. 3

'236	Russ(EX1005)
	<div data-bbox="600 262 1339 1071" data-label="Diagram"> </div> <div data-bbox="925 1228 1096 1291" data-label="Caption"> <p>FIG. 3</p> </div> <div data-bbox="487 1302 1421 1396" data-label="Text"> <p>Regarding decrypting a service instance according to an ECM including a counter value and entitlement specifier:</p> </div> <div data-bbox="511 1407 1453 1890" data-label="List-Group"> <ul style="list-style-type: none"> • 13:12-34 (<i>see</i> claim 130[c.iii]) • 13:35-39 (“entitlement generator 236 associates each encrypted service instance, with <u>a unique entitlement specifier, which is included in the ECM. A DSCT 110 uses the entitlement specifier to determine whether the DSCT 110 is entitled to the service instance.</u>”) • 15:46-52 (<i>see</i> claim 130[b.ii]) • 23:25-46 (“Each encrypted service instant is associated with an element in the entitlement array. <u>The entitlement specifier, which is included in the ECM for a given service</u> </div>

'236	Russ(EX1005)
	<p><u>instance, is used for determining an array element that has the entitlement of the DSCT 110 for the given service instance....</u></p> <p><u>When a user selects a service instance, the secure element 314 determines whether the DSCT 110 is entitled to the service instance. The AEMM 720 receives the ECM that is associated with the selected service instance, and authenticates the ECM. The ECM includes the entitlement specifier, a control word indicator (the counter value) and an authentication token, which is a hash digest of the control word indicator and a shared secret.”)</u></p> <ul style="list-style-type: none"> • 23:60-67 (“<u>The AEMM 720 uses the entitlement specifier of the ECM and the entitlements 714 to determine the DSCT's entitlement. Only if the DSCT 110 is entitled, does the secure element 314 to provide the cryptographic device 318 with the control word for decrypting the service instance. In the preferred embodiment, encrypting the control word indicator using the MSK as the encryption key generates the control word.</u>”) <p>See also:</p> <ul style="list-style-type: none"> • 13:3-11, 15:27-32, 23:47-54
<p>134[c]. wherein the access controlled data comprises a result of descrambling the scrambled content.</p>	<p>Russ discloses that the access controlled data comprises a result of descrambling the scrambled content (<i>e.g.</i>, DSCT 110 encrypts and transmits the decrypted service instance to client-receiver 122).</p> <p>Russ discloses descrambling or decrypting the service instance, as discussed for claim 134[b]. Russ further discloses the decrypted service instance is encrypted according to the encryption scheme determined between DSCT 110 and client-receiver 122 and then transmitted to client-receiver 122. Russ, Fig. 6, 15:46-52, 16:64-17:14, 19:50-20:19. Wasilewski, ¶¶124-126.</p> <p><i>E.g.,</i></p> <p>Regarding descrambling the scrambled content and encrypting the result for client-receiver 122:</p>

'236	Russ(EX1005)
	<ul style="list-style-type: none"> 15:46-52 (<i>see</i> claim 130[b.ii]) 16:64-17:14 (<i>see</i> claim 130[b.ii]) Fig. 6 <div data-bbox="600 434 1334 1421"> <pre> graph TD 602[RECEIVE SERVICE INSTANCE] --> 604{IS SERVICE INSTANCE ENCRYPTED?} 604 -- YES --> 606{DECRYPT SERVICE INSTANCE?} 604 -- NO --> 610{ENCRYPT SERVICE INSTANCE?} 606 -- YES --> 608[DECRYPT SERVICE INSTANCE] 606 -- NO --> 614[TRANSMIT SERVICE INSTANCE] 610 -- YES --> 612[ENCRYPT SERVICE INSTANCE] 610 -- NO --> 614 608 --> 610 612 --> 614 </pre> <p>The flowchart, labeled 600, illustrates a process for handling service instances. It begins with a rectangular box 602 labeled 'RECEIVE SERVICE INSTANCE'. An arrow points down to a diamond-shaped decision box 604 labeled 'IS SERVICE INSTANCE ENCRYPTED?'. From box 604, a 'YES' path leads right to a second diamond-shaped decision box 606 labeled 'DECRYPT SERVICE INSTANCE?'. From box 606, a 'YES' path leads left to a rectangular box 608 labeled 'DECRYPT SERVICE INSTANCE', which then leads down to a third diamond-shaped decision box 610 labeled 'ENCRYPT SERVICE INSTANCE?'. From box 604, a 'NO' path leads down directly to box 610. From box 610, a 'YES' path leads down to a rectangular box 612 labeled 'ENCRYPT SERVICE INSTANCE', which then leads down to a final rectangular box 614 labeled 'TRANSMIT SERVICE INSTANCE'. From box 610, a 'NO' path leads left and then down to box 614. A long arrow also points from box 602 directly to box 614, bypassing the encryption/decryption steps.</p> </div> <p style="text-align: center;">FIG. 6</p> <ul style="list-style-type: none"> 19:50-20:19 (<i>see</i> claim 130[c.iii]) <p>See also:</p> <ul style="list-style-type: none"> claim 19

135[pre]. The conditional access server	<i>See claim 134.</i>
---	-----------------------

'236	Russ(EX1005)
of claim 134, further comprising:	
<p>135[a] a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form;</p>	<p>Russ discloses a storage device coupled to one or more communication interfaces (<i>e.g.</i>, storage device 324 is connected to input-port 302, tuner 304, transceiver 308, client-receiver interface 320, output port 322), the storage device to store the content in an encrypted form (<i>e.g.</i>, service instances are stored on storage device 324; service instances are encrypted).</p> <p>Russ discloses that DSCT 110 includes storage device 324 for storing service instances for later retrieval. Russ, 15:55-62, 19:35-39, 19:45-49. Optionally, storage device 324 is external storage connected through output-port 322. Russ, 15:55-62. Stored service instances retrieved are encrypted. Russ, 15:16-26, 19:45-54. Wasilewski, ¶¶128-131.</p> <p><i>E.g.</i>,</p> <p>Regarding storage storing service instances:</p> <ul style="list-style-type: none"> • Fig. 3

'236	Russ (EX1005)
------	---------------

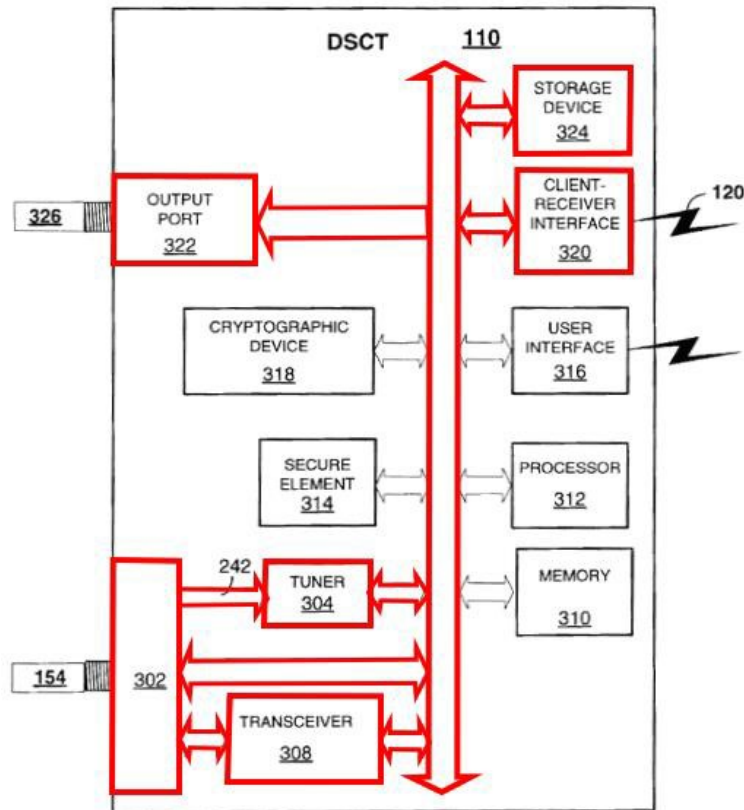


FIG. 3

- 15:55-62 (“The DSCT 110 also includes a storage device 324 for storing service instances.... In another embodiment, the storage device is external to the DSCT 110, and in that case, the service instance is sent to the external storage device through output-port 322 or through an input/output interface (not shown).”)
- 19:35-39 (“[W]hen the DSCT 110 receives a service request..., the DSCT 110 determines whether to provide the requested service to the client-receiver based upon local availability of the requested service.”)
- 19:45-54 (“[T]he selected service instance is stored on storage device 324 and is retrieved therefrom.
In step 604, the processor 312... determine[s] whether or

'236	Russ(EX1005)
	<p>not <u>the service instance is encrypted</u>. If <u>the selected service instance was encrypted</u> at the headend, the processor 312 determines... whether the service instance should be decrypted.”)</p> <p>Regarding service instances being encrypted:</p> <ul style="list-style-type: none"> • 15:16-26 (“<u>Frequently, the transport stream 242 includes some service instances that are not encrypted and some that are encrypted....</u> [I]f the selected service instance is encrypted, the processor 312 instructs the tuner 304 to send the selected service instance to the cryptographic device 318.”) • 19:45-54 (<i>see above</i>) <p>See also:</p> <ul style="list-style-type: none"> • 13:12-14, 18:16-28, 19:47-65
<p>135[b]. wherein the access controlled data is provided in response to a request from the secondary conditional access client.</p>	<p>Russ discloses that the access controlled data is provided in response to a request from the secondary conditional access client (<i>e.g.</i>, DSCT 110 transmits the EMM and service instance to client-receiver 122 in response to a request). Wasilewski, ¶¶132-134.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none"> • Fig. 5

'236	Russ(EX1005)
	<div data-bbox="597 256 1338 1050" data-label="Diagram"> <pre> graph TD 502[RECEIVE SERVICE REQUEST] --> 504{IS C-R ENTITLED?} 504 -- NO --> 510[PROVIDE C-R WITH ENTITLEMENT] 504 -- YES --> 506{IS SERVICE ACCESSIBLE?} 506 -- YES --> 512[PROVIDE C-R WITH SERVICE INSTANCE] 506 -- NO --> 508[SEND REQUEST FOR SERVICE] 508 --> 512 </pre> </div> <p style="text-align: center;">FIG. 5</p> <ul style="list-style-type: none"> 17:61-18:66 (“<u>In step 502, the DSCT 110 receives a request from the client-receiver 122 for a service instance.</u> In step 510.... secure element 314 generates an EMM... and sends the entitlement to the client-receiver 122.... <u>In step 512, the selected service instance is provided to the client-receiver 122.</u>”) See also 19:35-42, 19:50-20:19 (see claim 130[c.iii]), 20:22-24.

3. Claim Charts (32-34, 38-39, 66-68, 72-73)

Independent claim 32 and its dependent claims are directed to method steps (and related structures) that are substantially similar to the functions and steps related to the structures and elements of independent server claim 130 and its dependent claims. Similarly, independent claim 66 and its dependent claims are directed to program instructions causing a system to perform method steps that are substantially similar to the functions and steps in independent server claim 130 and its dependent claims. The claims are therefore disclosed for the same reasons identified above and as identified in the chart below. Wasilewski, ¶¶135-183.

'236	Russ(EX1005)
32[pre]. A method to process conditional access protection, the method comprising:	<i>See</i> claim 130. The conditional access server (<i>e.g.</i> , DSCT 110) processes conditional access protection (<i>e.g.</i> , providing service instances and entitlements to client-receiver 122). Wasilewski, ¶¶136-138.

32[a]. receiving, at a conditional access server, security messages of a primary security system in a first security domain;	<i>See claim 130[pre]-130[a].</i>
32[b]. processing the	<i>See claim 130[b.i].</i>

'236	Russ(EX1005)
security messages on the conditional access server; and	
32[c]. transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,	<i>See claim 130[b.ii].</i>

32[d.i]. wherein the primary security system authenticates the conditional access server as one of clients of the primary security system	<i>See claim 130[c.i].</i>
--	----------------------------

'236	Russ(EX1005)
through a first authentication process using a first root of trust and	
32[d.ii] the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and	<i>See claim 130[c.ii].</i>

32[d.iii] wherein the conditional access server is configured to substitute the first security domain with	<i>See claim 130[c.iii].</i>
--	------------------------------

'236	Russ(EX1005)
the second security domain for the clients under the second root of trust.	
33[pre]. The method of claim 32, wherein	<i>See claim 32.</i>
33[a]. the security messages comprise entitlement management messages;	<i>See claim 131.</i>
33[b]. the conditional access server has a user key representing a subscriber of the primary security system; and	<p>Russ discloses that the conditional access server has a user key representing a subscriber of the primary security system (<i>e.g.</i>, DSCT 110 includes a private key used to decrypt communications from headend 102; the private key represents a subscriber of the primary system because it uniquely grants access to content from headend 102, with whom DSCT 110 is registered). Wasilewski, ¶¶147-149.</p> <p><i>E.g.,</i></p> <ul style="list-style-type: none"> • 7:7-13 (“headend 102 includes a database... that has the public key of each DSCT 110.... <u>The headend 102 can securely communicate with a particular DSCT 110 by encrypting the content of a message using the public key of the particular DSCT 110. Only the particular DSCT 110 that has the corresponding private key can decrypt the content of the message.</u>”) • 7:56-58 (<i>see</i> claim 130[a]) • 20:34-46 (“keys 710 include a public key-private key pair for the DSCT 110.... <u>The private key of the DSCT 110 is stored in the memory 704....</u> The holders of the DSCT's public key can use the public key... for encrypting

'236	Russ(EX1005)
	messages sent to the DSCT 110.”)
<p>33[c]. said processing the entitlement management messages comprises: decrypting to obtain a service key of the primary security system.</p>	<p>Russ discloses that processing the entitlement management messages comprises decrypting to obtain a service key of the primary security system (<i>e.g.</i>, secure element 314 decrypts EMMs to obtain MSKs).</p> <p>Russ discloses that EMMs contain a multi-session key (MSK) of headend 102; the MSK is a key used to generate control words for decrypting service instances. Russ, 11:37-46, 13:12-34. EMMs are encrypted, and DSCT 110 includes secure element 314, which includes AEMM 720 and which decrypts received EMMs to obtain the MSK. Russ, 10:48-65, 22:40-45. Wasilewski, ¶¶150-152.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none"> • 10:48-65 (<i>see</i> claim 130[a]) • 11:37-46 (<i>see</i> claim 130[c.iii]) • 13:12-34 (<i>see</i> claim 130[c.iii]) • 22:40-45 (“Referring again to FIG. 7, the AEMM 720 includes the logic for authenticating and decrypting a received EMM 800. If the EMM is encrypted, the AEMM 720 uses the private key of the DSCT 110 to decrypt the message content....”)
<p>34. The method of claim 32, wherein the access controlled data is protected using a digital rights management system.</p>	<p><i>See</i> claim 131.</p>
<p>38[pre]. The method of claim 34,</p>	<p><i>See</i> claim 34.</p>

'236	Russ(EX1005)
further comprising:	
38[a]. receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and	<i>See claim 134[a].</i>
38[b]. descrambling the scrambled content according to the entitlement control message;	<i>See claim 134[b].</i>
38[c]. wherein the access controlled data comprises a result of descrambling the scrambled content.	<i>See claim 134[c].</i>
39[pre]. The method of claim 38, further comprising:	<i>See claim 38.</i>

39[a]. storing, at the conditional	<i>See claim 135[a].</i>
---	--------------------------

'236	Russ(EX1005)
access server, the content in an encrypted form;	
39[b]. wherein the access controlled data is provided in response to a request from the secondary conditional access client.	<i>See</i> claim 135[b].
66[pre]. A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, the method comprising:	<p>Russ discloses a non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method (<i>e.g.</i>, software stored in memory and executed by a processor, secure element, and cryptographic device to implement logic steps) to process conditional access protection (<i>e.g.</i>, to perform conditional access server methods; <i>see</i> claims 32, 130). Wasilewski, ¶¶162-165.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none"> • 3:23-40 (“The logic of the preferred embodiment(s)... 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>.”) • <i>See also</i> 16:13-26 and 17:61-62 and 19:43-45 (describing logic in processor 312, secure element 314, and cryptographic device 318).

'236	Russ(EX1005)
66[a]. receiving, at a conditional access server, security messages of a primary security system in a first security domain;	<i>See claim 130[pre]-130[a].</i>
66[b]. processing the security messages on the conditional access server; and	<i>See claim 130[b.i].</i>

66[c]. transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from	<i>See claim 130[b.ii].</i>
---	-----------------------------

'236	Russ(EX1005)
the security messages,	
66[d.i] wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and	<i>See claim 130[c.i].</i>

66[d.ii] the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is	<i>See claim 130[c.ii].</i>
--	-----------------------------

'236	Russ(EX1005)
independent of and different than the first root of trust, and	
66[d.iii] wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.	<i>See claim 130[c.iii].</i>
67[pre]. The medium of claim 66, wherein	<i>See claim 66.</i>
67[a]. the security messages comprise entitlement management messages;	<i>See claim 131.</i>

67[b]. the conditional access server has a user key representing a subscriber of the primary security system; and	<i>See claim 33[b].</i>
--	-------------------------

'236	Russ(EX1005)
<p>67[c]. said processing the entitlement management messages comprises: decrypting to obtain a service key of the primary security system.</p>	<p><i>See claim 33[c].</i></p>
<p>68. The medium of claim 66, wherein the access controlled data is protected using a digital rights management system.</p>	<p><i>See claim 131.</i></p>
<p>72[pre.] The medium of claim 68, wherein the method further comprises:</p>	<p><i>See claim 68.</i></p>

72[a]. receiving, at the conditional access server, an entitlement control message and scrambled content of the primary	<i>See claim 134[a].</i>
---	--------------------------

'236	Russ(EX1005)
security system; and	
72[b]. descrambling the scrambled content according to the entitlement control message;	<i>See claim 134[b].</i>
72[c]. wherein the access controlled data comprises a result of descrambling the scrambled content.	<i>See claim 134[c].</i>
73[pre]. The medium of claim 72, wherein the method further comprises:	<i>See claim 72.</i>
73[a]. storing, at the conditional access server, the content in an encrypted form;	<i>See claim 135[a].</i>

73[b]. wherein the access controlled data is provided in response to a request from	<i>See claim 135[b].</i>
--	--------------------------

'236	Russ(EX1005)
the secondary conditional access client.	

B. Ground 2: Claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 are Obvious Over Russ

Russ anticipates claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 as discussed in §VII.A. Wasilewski, ¶¶185-186. To the extent PO argues that various relied-on features of Russ 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, 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 alterations 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, ¶187.

Accordingly, in light of the structures and functions identified in the claim charts in §VII.A.2-VII.A.3, which also apply here, claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 are obvious over Russ. Wasilewski, ¶188.

C. Ground 3: Claims 35-36, 69-70, and 132-133 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 different than a content protection scheme with which it originated. EX1006 (“Robert”), Abstract, 2:23-33, 6:17-30. To do so, Robert discloses transcribing content protection information from one syntax to the other. Robert, 6:26-30. Wasilewski, ¶¶59-61.

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.

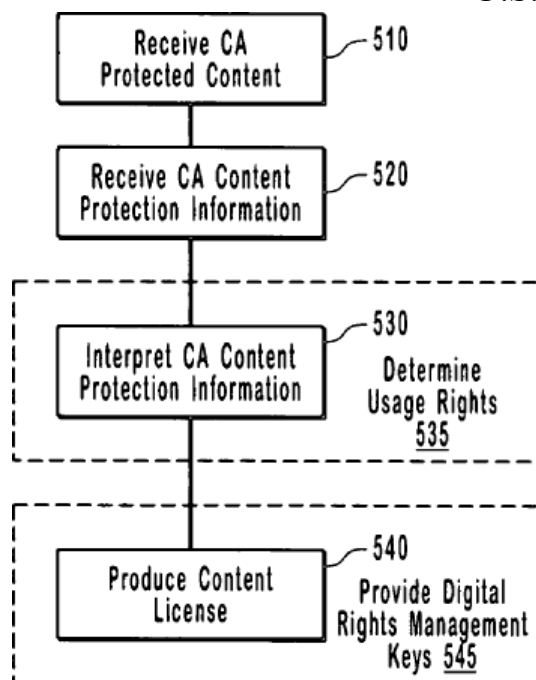


Fig. 5

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, ¶60.

Variations on the steps 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 steps at different times and devices. Robert, 6:26-59. Wasilewski, ¶61.

2. *Motivation: Russ in view of Robert*

Russ and Robert are in the same field as the '236—*e.g.*, content protection schemes. '236, 1:5-2:53. *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, ¶65.

As explained in §VII.A, 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 nown method to use for protected communication between **DSCT 110** and **client-receiver 122** and does not explicitly recite all details—for example how **client-receiver 122's** entitlements to service instances are determined (*e.g.*, with respect to claim 132) or for example what specific control words client-receiver 122 uses to decrypt service instances (*e.g.*, with respect to claim 133). 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 derive rights to access controlled data from EMMs and to transmit control words from **DSCT 110** to **client-receiver 122** in Russ, as taught by Robert, for the reasons below. Wasilewski, ¶189.

Regarding claim 132, Russ discloses that **DSCT 110** receives an entitlement for a service instance in an EMM, then processes the EMM and provides the

entitlement to **client-receiver 122**. Russ, 18:60-19:6. However, Russ leaves to the POSA specific implementation details regarding entitlements or usage rights for the myriad of encryption schemes that may be selected for communications between **DSCT 110** and **client-receiver 122**, like DTCP or CPRM DRM schemes. Russ, 16:64-17:14. Robert teaches exemplary examples of systems for accessing CA protected content on devices requiring DRM licenses and protection. Robert, 8:56-11:59. For example, Robert teaches interpreting content protection information for the CA content to determine usage rights, producing a content license according to those usage rights, and then providing DRM keys to a destination device with those rights. Robert, 12:16-26. By interpreting and deriving rights from the original protection information, the system “maintain[s] security of the content and any associated protection content information (e.g., usage rights, access conditions, encryption keys, etc.).” Robert, 4:50-65, 6:19-26. A POSA would have therefore been motivated to implement Russ with the implementation details taught by Robert and provide rights to services instances, transmitted to **client-receiver 122** via DTCP protocols, that are derived from the entitlement received at **DSCT 110**, so that rights are not lost or evaded between **headend 102**, **DSCT 110**, and finally at the subscriber location’s **client-receiver 122**. Wasilewski, ¶190.

Regarding claim 133, 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, the **destination device** can use a DRM license to decrypt CA-protected content. Robert, 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, ¶191.

Furthermore, the implementations above would have been, at least, the application of known techniques (*e.g.*, Robert's teachings of deriving rights to access controlled data and 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 deriving rights from EMMs and 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 rights and control words of known content protection schemes, on known computing devices, requires only data processing techniques well within the skill of a POSA. Wasilewski, ¶192.

3. *Claim Charts (132-133)*

'236	Russ(EX1005)+Robert(EX1006)
<p>132. The conditional access server of claim 131, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.</p>	<p>Russ discloses that rights to the access controlled data are at least partially derived from the entitlement management messages (<i>e.g.</i>, DSCT 110 receives service instance entitlements in the EMM, then provides entitlements to client-receiver 122). Wasilewski, ¶194.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none"> • 17:61-18:66 (<i>see</i> claim 130[pre] in §VII.A.2; DSCT 110 grants entitlements to client-receiver 122) • 18:52-65 (<i>see</i> claim 130[b.ii] in §VII.A.2) • <i>See also</i> 16:64-17:14, 21:11-21, 24:1-24, 21:22-65. <p>Robert discloses that rights to the access controlled data are at least partially derived from the entitlement management messages (<i>e.g.</i>, a receiving device receives content protection information in an EMM from a content provider in a conditional access system, interprets the content protection information to determine usage rights, and translates the content protection information for a destination device using a DRM system).</p> <p>In addition to Russ's disclosures that entitlements received via EMM at DSCT 110 are processed and provided to client-receiver 122, whose communications are protected by the dynamically determined encryption scheme such as DTCP as discussed in at least claims 130[c.ii]-[c.iii], Robert teaches translating content from one content protection scheme to another by interpreting and transcribing content protection information into a usage rights license. Robert, 12:8-26. A</p>

'236	Russ(EX1005)+Robert(EX1006)
------	-----------------------------

POSA would have been motivated to derive client-receiver 122's rights to service instances by interpreting received EMMs, as taught by Robert, as discussed in §VII.C.2. Wasilewski, ¶195; ¶¶193-196.

E.g.,

- Fig. 5

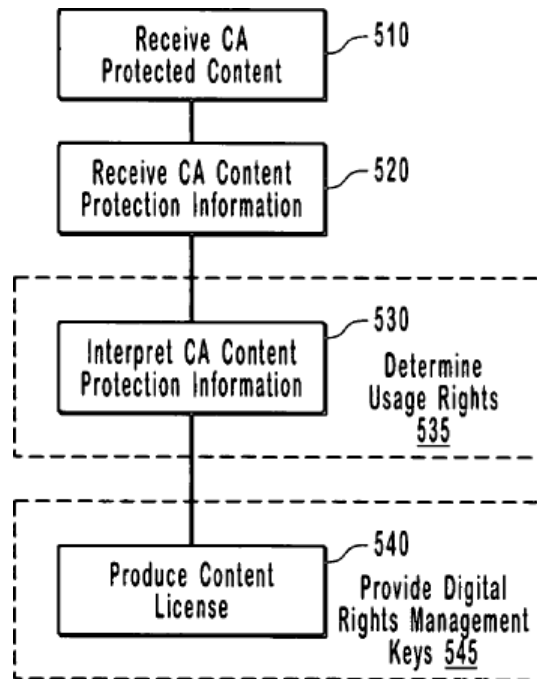
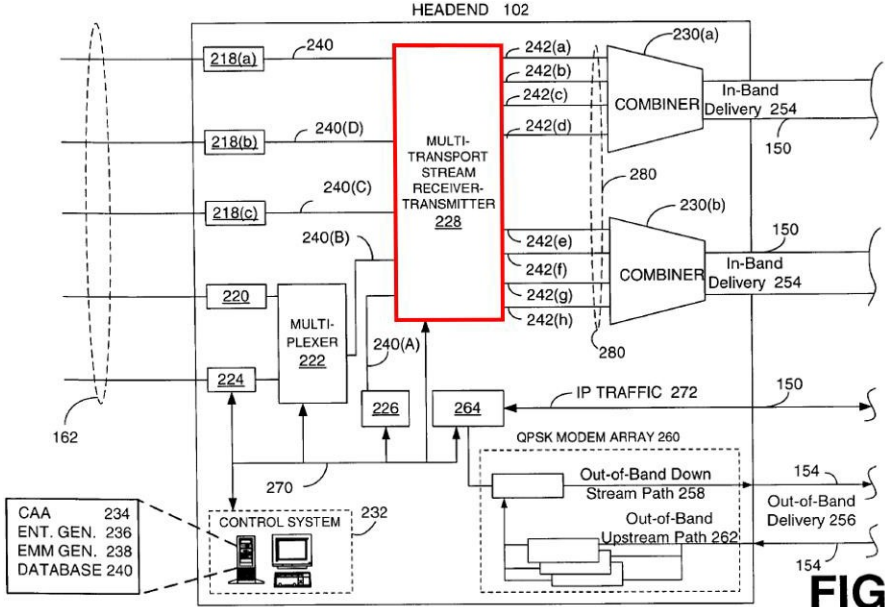


Fig. 5

- 12:8-26 (“[C]onditional access-protected content and content protection information are received in acts 510 and 520, respectively. The conditional access-protected content is... encrypted by a plurality of intermittent updated keys. Further, the content protection information includes information used to determine, manage and enforce usage rights associated with the conditional access-protected content.”)

[A] step for determining 535 usage rights may include the acts of interpreting 530 CA content protection information. The usage rights... specify how and under what conditions content may consumed at a destination device.

'236	Russ(EX1005)+Robert(EX1006)
	<p><u>A step for providing 545 digital rights management keys may include the act of producing 540 a content license used for enforcing digital rights within the destination device. Of course, information within the license is based upon the interpreted conditional access content protection information and in accordance with usage rights.”)</u></p> <ul style="list-style-type: none"> • <i>See also</i> 2:23-33, 4:18-26 (describing EMMs providing control information), 6:31-59, 8:56-11:59 and Figs. 4A-4L (describing combinations of CA and DRM, and derivations of content protection information)
<p>133[pre]. The conditional access server of claim 131, wherein</p>	<p><i>See</i> claim 131 in §VII.A.2.</p>
<p>133[a]. the one or more communication interfaces are to receive an entitlement control message of the primary security system;</p>	<p><i>See</i> claim 134[a] in §VII.A.2.</p>
<p>133[b]. the processor is to obtain a control word of the primary security system from the entitlement control</p>	<p>Russ discloses that the processor is to obtain a control word of the primary security system from the entitlement control message (<i>e.g.</i>, DSCT 110 encrypts a control word indicator of the ECM to obtain a control word generated by entitlement generator 236 of headend 102).</p> <p>Russ discloses that service instances are encrypted by headend 102 with a control word based on a control word indicator (or counter value). Russ, 11:37-46, 13:12-19. The control word</p>

'236	Russ(EX1005)+Robert(EX1006)
<p>message; and</p>	<p>indicator is included in the ECM received by DSCT 110. Russ, 23:39-46. When DSCT 110 is entitled to a service instance, its secure element 314 generates a control word from the control word indicator and provides the control word to cryptographic device 318. Russ, 23:55-67. Wasilewski, ¶¶199-201.</p> <p><i>E.g.,</i></p> <ul style="list-style-type: none"> Fig. 2  <p style="text-align: right;">FIG. 2</p> <ul style="list-style-type: none"> 11:37-46 (<i>see</i> claim 130[c.iii] in §VII.A.2) 13:12-34 (<i>see</i> claim 130[c.iii] in §VII.A.2) 23:25-46 (<i>see</i> claim 134[b] in §VII.A.2) 23:60-67 (<i>see</i> claim 134[b] in §VII.A.2) <i>See also</i> 11:37-46, 13:12-19.
<p>133[c]. the access controlled data comprises the control word.</p>	<p>Robert discloses that the access controlled data comprises the control word (<i>e.g.</i>, a receiver receiving a control word in a controlled access system transmits the control word to the destination device protected via DRM).</p> <p>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</p>

'236	Russ(EX1005)+Robert(EX1006)
	<p>client-receiver 122 and Robert's destination device 420) in a DRM license sent to the device. 9:66-10:4. A POSA would have been motivated to implement Russ by transmitting the control word to client-receiver 122 as access controlled data, as taught by Robert, as discussed in §VII.C.2. Wasilewski, ¶¶202-205.</p> <p><i>E.g.,</i></p> <ul style="list-style-type: none"> 6:31-59 (“[T]here 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..., 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 to be used to decrypt the encoded conditional access content.</u>”) 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) <div data-bbox="500 1171 1433 1497"> <p>The diagram illustrates the process of content protection information flow. On the left, a 'Receiver' (410) is shown as a blue box containing three sub-components: 'CASD', 'CAK', and 'SCK'. Three inputs enter the Receiver from the left: 'ECM' (405), 'EMM' (405), and 'E_CW[content]' (425). From the Receiver, two outputs are shown: a 'DRM License' (430) and 'E_CW[content]' (425). These outputs are directed towards a 'Destination Device' (420), represented by a computer monitor and keyboard. The Destination Device then produces two possible outputs: 'E_CW[content]' (425) or 'E_KC[content]' (435).</p> </div> <p>Fig. 4C</p> <ul style="list-style-type: none"> 9:53-10:4 (“FIG. 4C illustrates... producing a content license 430 used to consume content 425, 435 in accordance with usage rights defined by CPI in a CA system. Again, receiver 410, which is a CASD..., receives CAM 405 and CA-protected content 425. In this implementation..., receiver 410 is capable of producing or generating DRM license 430 and sending such license 430 to the destination DRM device 420.... [R]eceiver 410 <u>could have included the appropriate keys (e.g., a list of</u>

'236	Russ(EX1005)+Robert(EX1006)
	<u>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 form.”)</u>

4. Claim Charts (35-36, 69-70)

See discussion of claims 32 and 66 and their dependents in §VII.A.3.

'236	Russ(EX1005)+Robert(EX1006)
35. The method of claim 34, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.	See claim 132.
36[pre]. The method of claim 34, further comprising:	See claim 34.
36[a]. receiving, at the conditional access server, an entitlement control message of the primary security	See claim 134[a].

'236	Russ(EX1005)+Robert(EX1006)
system; and	
36[b]. processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;	<i>See claim 133[b].</i>
36[c]. wherein the access controlled data comprises the control word.	<i>See claim 133[c].</i>
69. The medium of claim 68, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.	<i>See claim 132.</i>
70[pre]. The medium of claim 68, wherein the method further comprises:	<i>See claim 68.</i>

70[a]. receiving, at	<i>See claim 134[a].</i>
--------------------------------	--------------------------

'236	Russ(EX1005)+Robert(EX1006)
the conditional access server, an entitlement control message of the primary security system; and	
70[b]. processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;	See claim 133[b].
70[c]. wherein the access controlled data comprises the control word.	See claim 133[c].

D. Ground 4: Claims 40-41, 43, 74-75, 77, and 136-137 are Obvious Over Russ in view of Eskicioglu

1. Overview: Eskicioglu

Eskicioglu describes a copy protection system that provides security during transmission and storage of content. EX1007 (“Eskicioglu”), Abstract, 1:15-20. Eskicioglu explains that home networks must protect against illegal copying and distribution and not only ensure that viewing is permitted.

Eskicioglu, 1:24-60. Fig. 1A below shows an exemplary system in which

content flows from a **source** (e.g., cable) to an **access device 14** (e.g., set-top

box) to a **presentation device 16** (e.g., television). Eskicioglu, 3:13-21, 4:16-

45. Wasilewski, ¶¶62-63.

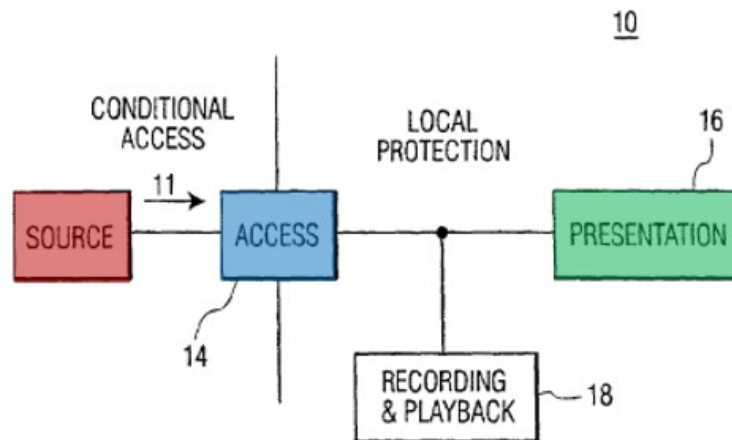


FIG. 1A

Eskicioglu discloses local protection within a home network by rebundling keys required for descrambling content, from an ECM into a local ECM (“LECM”) protected by a unique key. Eskicioglu, 2:1-40. In Fig. 4 below, an ECM undergoes a translation process 42 (at **access device 14**, which includes a security device 26) for rebundling into the LECM. Eskicioglu, 8:4-10. While the ECM is protected by a key associated with a service provider, the LECM is protected by a local public key. Eskicioglu, 2:1-40, 7:41-53, 8:4-18.

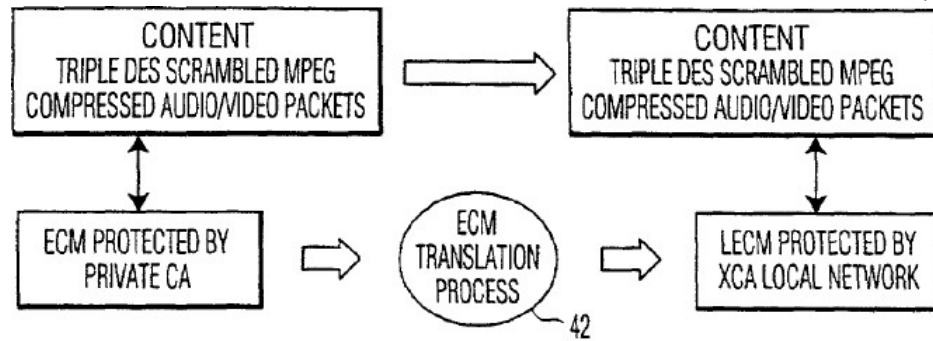


FIG. 4

Presentation device 16 with the rebundled LECM is therefore able to descramble and view content. Eskicioglu, Fig. 5, 8:10-16, 8:30-47, 11:41-58, 12:24-43.

Wasilewski, ¶64.

2. *Motivation: Russ in view of Eskicioglu*

Russ and Eskicioglu are in the same field as the '236—*e.g.*, content protection schemes. *See* §VII.C.2; Eskicioglu, 1:15-60 (providing security of audio and video content during transmission and storage). Wasilewski, ¶65.

As explained in §VII.A, 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**.

Eskicioglu teaches one known method for providing content and content protection information across different content protection schemes with substitutive ECMs that contain control words, thus providing security specific to a local network. Eskicioglu, 2:1-40, 8:4-18. It would have been obvious to a POSA to implement Russ using substitutive ECMs for **client-receiver 122** in the local network, as taught by Eskicioglu, for the reasons below. Wasilewski, ¶217.

As discussed in §VII.C.2, Russ discloses that **client-receiver 122** decrypts service instances by generating control words and does not explicitly explain the origin of those control words, but explains that **DSCT 110** and **client-receiver 122** communicate with negotiated protocols and encryption in one of any number of schemes known to POSAs. Russ, 16:64-17:60, 20:12-17, 26:16-28, 26:34-37, 26:54-67. Eskicioglu teaches one variety, extended conditional access (“XCA”), for protecting received CA content in local networks. Eskicioglu, 1:16-20, 2:1-40, 2:65-3:11, 3:50-4:15. In a system where CA content is received by an **access device** and destined for consumption at a **presentation device**, ECMs associated with the CA content and protected by a service providers’ keys, are rebundled into LECMs protected by a local public key. Eskicioglu, 2:1-40, 7:41-53, 8:4-18. A POSA would have therefore been motivated to implement Russ, which is otherwise open-ended for the POSA to decide which known encryption scheme to use between **DSCT 110** and **client-receiver 122**, by configuring **DSCT 110’s** secure element, which

processes security messages including ECMs (*see, e.g.*, the discussion of claims 130[b.i] and 133[b] above) to generate and transmit a substitutive ECM (or LECM) with a control word encrypted with **DSCT 110's** key, as taught by Eskicioglu, to protect content in the local network and to ensure that the content is protected and not accessed outside the local network. Eskicioglu, 8:10-18. As Russ discloses that the service instance may not need to be decrypted first by **DSCT 110** (*see* Russ, 19:50-59), use of the new LECM with the same service instance received from **headend 102** would have saved time and resources at **DSCT 110** while further substituting the primary security domain provided by **headend 102** (via the original ECM) with the secondary security domain provided by **DSCT 110** (via the LECM). Wasilewski, ¶218.

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

Eskicioglu's LECMs are structurally and functionally similar to well-known ECMs used in Russ. Additionally, the incorporation of ECM control words (*e.g.*, as taught by Eskicioglu) in DRM systems (*e.g.*, Russ discloses that **DSCT 110** communicates with client-receiver 122 using DTCP protocols) in various ways was a practice readily known to POSAs. *See* Russ, 17:7-14; Robert, 6:31-59. The use of an LECM data structure requires only data processing techniques well within the skill of a POSA. Wasilewski, ¶219.

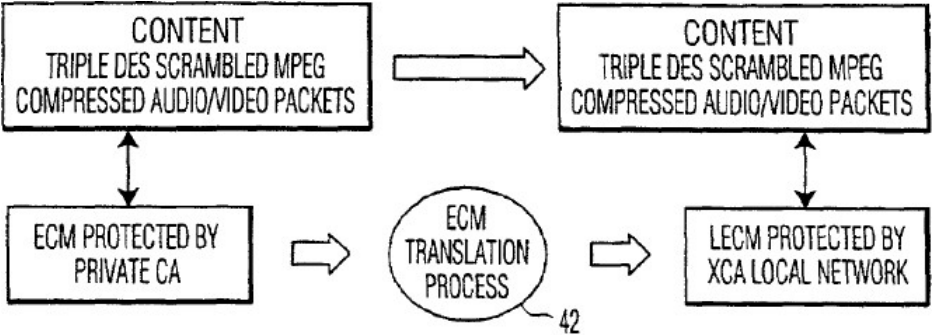
3. *Claim Charts (136-137)*

'236	Russ(EX1005)+Eskicioglu(EX1007)
136[pre]. The conditional access server of claim 130, wherein	<i>See</i> claim 130 in §VII.A.2.
136[a]. the one or more communication interfaces are to receive entitlement control message of the primary security system;	<i>See</i> claim 134[a] in §VII.A.2.

136[b]. the processor is to generate a substitutive entitlement	Eskicioglu discloses that the processor (<i>e.g.</i> , security device 26) is to generate a substitutive entitlement control message as a replacement of the entitlement control message (<i>e.g.</i> , receiving an ECM, and processing the ECM to rebundle the ECM contents into a local ECM (“LECM”)); and the access
--	---

'236	Russ(EX1005)+Eskicioglu(EX1007)
control message as a replacement of the entitlement control message; and the access controlled data comprises the substitutive entitlement control message.	<p>controlled data comprises the substitutive entitlement control message (<i>e.g.</i>, the LECM is transmitted to the presentation device).</p> <p>In addition to Russ’s disclosures of DSCT 110 re-encrypting information for client-receiver 122 based on a dynamically determined encryption scheme—which may include any known protection protocols known to POSAs and which, in one example, client-receiver 122 decrypts information to generate control words to decrypt a service instance (<i>see</i> Russ, 16:64-17:14, 26:16-28, 26:54-67)—but does not explicitly describe DSCT 110 generating a substitutive ECM for client-receiver 122, Eskicioglu teaches access device functionality including processing ECMs to generate substitutive local ECMs (LECMs) transmitted to presentation devices for descrambling content, which would have been obvious to a POSA to implement in Russ, as discussed in §VII.D.2. Eskicioglu, 2:1-10, 7:41-53, 8:4-12, claim 1. Wasilewski, ¶¶222-225.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none">Fig. 1A (access device 14 receiving conditional access content that is to be presented locally on presentation device 16) <p>The diagram, labeled FIG. 1A, illustrates a system architecture. A red box labeled 'SOURCE' is connected by an arrow labeled '11' to a blue box labeled 'ACCESS'. The 'ACCESS' box is also connected to a green box labeled 'PRESENTATION' and a white box labeled 'RECORDING & PLAYBACK'. A vertical line passes through the 'ACCESS' box, with the label 'CONDITIONAL ACCESS' above it and '14' below it. Another vertical line passes through the 'PRESENTATION' box, with the label 'LOCAL PROTECTION' above it and '16' below it. The 'RECORDING & PLAYBACK' box is connected to the line between 'ACCESS' and 'PRESENTATION' and is labeled '18'.</p> <p>FIG. 1A</p>

- | | |
|--|--|
| | <ul style="list-style-type: none">• 4:46-50 (“Access devices typically operate in combination with an XCA/NRSS Converter Card.... The XCA/NRSS converter card creates XCA protected content from private |
|--|--|

'236	Russ(EX1005)+Eskicioglu(EX1007)
	<p>conditional access (CA) protected content...”)</p> <ul style="list-style-type: none"> 7:41-46 (“<u>The keys for content descrambling are rebundled in LECMs by access device 14. That is, the encrypted ECMs, which carry the descrambling keys, are decrypted by access device 14 and then re-encrypted using a local public key associated with the access device to produce the LECM.</u>”) Fig. 4  <p style="text-align: center;">FIG. 4</p> <ul style="list-style-type: none"> 8:4-12 (“As shown in FIG. 4, XCA protects the content on the local network by <u>rebundling (i.e., ECM translation) 42 the keys required for descrambling (i.e., the TDES keys) into a new ECM which is protected by a local public key associated with the access device (i.e., LECM). This process is typically performed in access device 14 and preferably in security device 26. In this fashion, the only device capable of recovering the TDES keys and hence descrambling the MPEG program is the local presentation device, e.g., DTV.</u>”) Claim 1 (“ (a) <u>receiving... said scrambled program comprising a scrambled data component and an encrypted descrambling key;</u> (b) <u>rebundling... said descrambling key using a unique key associated with said first device, wherein said first</u>

'236	Russ(EX1005)+Eskicioglu(EX1007)
	<p>device is an access device;</p> <p>(c) <u>receiving, in said second device</u>, said scrambled data component and <u>said rebundled descrambling key...</u>")</p> <ul style="list-style-type: none"> • See also Fig. 5, 2:1-10, 4:25-27, 4:57-5:3, 8:19-47.
<p>137. The conditional access server of claim 136, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.</p>	<p>See claim 136.</p> <p>Eskicioglu discloses that the substitutive entitlement control message has a control word (e.g., the LECM is a rebundled ECM, including control words) encrypted using a key of the conditional access server (e.g., the LECM is encrypted with the public key associated with the access device).</p> <p>Eskicioglu discloses that the LECM includes control words (or equivalent keys) for descrambling content. Eskicioglu, 2:3-7, 7:41-53. The LECM contents are encrypted with a unique key associated with the conditional access server—<i>i.e.</i>, associated with a “first”/“access” device 14 that receives the content and ECM and rebundles the ECM into the LECM. Eskicioglu, 2:3-7, 7:41-46, 8:19-30. Wasilewski, ¶¶226-228.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none"> • 2:3-7 (“This method may comprise receiving a scrambled program (e.g., a scrambled data component and a descrambling key) in the first device, and <u>rebundling the descrambling key using a unique key associated with the first device.</u>”) • 7:41-46 (<i>see</i> claim 136) • Fig. 5

'236	Russ(EX1005)+Eskicioglu(EX1007)
	<p style="text-align: center;">FIG. 5</p> <ul style="list-style-type: none"> 8:19-30 (“The flow of content with the XCA domain is further explained using FIG. 5.... <u>CA module 42 recovers the control words (CW) or keys for the CA content and passes the CWs to converter module 46 which generates the necessary LECM.</u>”) See also Fig. 5, 4:57-5:3, 8:4-47, claim 1.

4. Claim Charts (40-41, 43, 74-75, 77)

See discussion of claims 32 and 66 and their dependents in §VII.A.3.

'236	Russ(EX1005)+Eskicioglu(EX1007)
40[pre]. The method of claim 32, further comprising:	See claim 32.

40[a]. receiving, at the conditional	<i>See</i> claim 134[a].
---	--------------------------

'236	Russ(EX1005)+Eskicioglu(EX1007)
access server, an entitlement control message of the primary security system; and	
40[b]. processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message; wherein the access controlled data comprises the substitutive entitlement control message.	<i>See claim 136[b].</i>

41. The method of claim 40, wherein the substitutive entitlement control message has a	<i>See claim 137.</i>
--	-----------------------

'236	Russ(EX1005)+Eskicioglu(EX1007)
control word encrypted using a key of the conditional access server.	
<p>43. The method of claim 41, wherein the entitlement control message and the substitutive entitlement control message have a same control word.</p>	<p>Eskicioglu discloses that the entitlement control message and the substitutive entitlement control message have a same control word (e.g., the ECM and LECM have a same control word).</p> <p>As discussed for claims 136[b] and 137, Eskicioglu discloses that the LECM includes control words (or equivalent keys) for descrambling content, which are obtained by decrypting the ECM. Eskicioglu, 1:66-2:10, 7:41-53. Eskicioglu does not disclose that the control words are altered—the LECM is a rebundling of the ECM. Eskicioglu, 8:4-12. The ECM and LECM therefore have the same control word. Wasilewski, ¶¶223-225.</p>
<p>74[pre]. The medium of claim 66, wherein the method further comprises:</p>	<p><i>See claim 66.</i></p>
<p>74[a]. receiving, at the conditional access server, an entitlement control message of the primary security system; and</p>	<p><i>See claim 134[a].</i></p>

74[b]. processing the entitlement control message on the	<i>See claim 136[b].</i>
---	--------------------------

'236	Russ(EX1005)+Eskicioglu(EX1007)
conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message; wherein the access controlled data comprises the substitutive entitlement control message.	
75. The medium of claim 74, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.	<i>See claim 137.</i>

77. The medium of claim 75, wherein the entitlement control message and	<i>See claim 43.</i>
--	----------------------

'236	Russ (EX1005) + Eskicioglu (EX1007)
the substitutive entitlement control message have a same control word.	

VIII. NO BASIS FOR DISCRETIONARY DENIAL

A. Fintiv

“Pursuant to the Director’s Memo, [the Board] ‘will not discretionarily deny institution ... where a petitioner presents a [*Sotera*] stipulation.” IPR2024-00099, Paper 11, at 21–22 (PTAB May 9, 2024).

Petitioner stipulates if the present proceeding is instituted and joined with the Roku IPR, it will not pursue in the district court litigation any ground that was raised or could have been reasonably raised in an IPR in accordance with *Sotera Wireless, Inc. v. Masimo Corporation*, IPR2020-1019, Paper 12 at 17-19 (P.T.A.B. Dec. 1, 202) (precedential, designated Dec. 17, 2020).

IX. CONCLUSION

The Board should institute IPR and cancel the Claims of the '236.

Dated: December 17, 2024 Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Eric A. Buresh
Eric A. Buresh, Reg. No. 50,394

IPR2025-00304

U.S. Patent No.8,291,236

eric.buresh@eriseip.com

7015 College Blvd., Suite 700

Overland Park, KS 66211

P: (913) 777-5600

F: (913) 777-5601

COUNSEL FOR PETITIONER

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,980 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: December 17, 2024

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Eric A. Buresh
Eric A. Buresh, Reg. No. 50,394
eric.buresh@eriseip.com
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER

**CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on December 17, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '236 Patent:

WORKMAN NYDEGGER
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

Further, a courtesy copy of this *Petition for Inter Partes Review* was sent via email to Petitioner's and Patent Owner's counsel for IPR2024-01023:

Scott A. McKeown (SMcKeown-
PTAB@WolfGreenfield.com)
Libbie A. DiMarco
(Elizabeth.DiMarco@WolfGreenfield.com)
Victor Cheung (VCheung-PTAB@WolfGreenfield.com)
Jerry D. Tice, II (jtice@bdiplaw.com)
Aaron R. Hand (ahand@bdiplaw.com)
VideoLabs_Roku@bdiplaw.com

Further, a courtesy copy of this *Petition for Inter Partes Review* was sent via email to Patent Owner's litigation counsel:

Massimo Ciccarelli (max@ciccarellilawfirm.com)
Andrew Tseng (andrew.tseng@troutman.com)
William D.Bellinger (William.bellinger@troutman.com)
Griffin N. Mesmer (griffin.messmer@troutman.com)
Gregory Len (gregory.len@troutman.com)
Ana Spone (ana.spone@troutman.com)
Frank D. Lieu (frank.lieu@troutman.com)
Ryan C. Deck (ryan.deck@troutman.com)

Respectfully submitted,

ERISE IP, P.A.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Eric A. Buresh
Eric A. Buresh, Reg. No. 50,394
eric.buresh@eriseip.com
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER