

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

VIDEOLABS, INC.,
Patent Owner.

Case No. IPR2025-00881
Patent No. 8,291,236

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

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	6
	A. Real Party-In-Interest	6
	B. Related Matters.....	7
	C. Lead and Back-up Counsel, and Service Information	8
III.	REQUIREMENTS FOR IPR	9
	A. Grounds for Standing (37 C.F.R. §42.104(a))	9
	B. Identification of Challenge (37 C.F.R. §42.104(b)).....	9
	1. Specific Art on Which the Challenge is Based.....	9
	2. Statutory Grounds on Which the Challenge is Based.....	9
IV.	BACKGROUND	10
	A. '236 Patent.....	10
	B. Prosecution History of the '236	13
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	14
VI.	CLAIM INTERPRETATION	15
	A. “access controlled data that is in an access controlled format and that is at least partially derived from a security message”	15
	B. Means-plus-function terms.....	17
	1. “means for receiving, at a secondary conditional access client”	18
VII.	GROUND OF UNPATENTABILITY.....	19
	A. Ground 1: Claims 48-50, 57, 82-84, 91, 116-118, 125, and 140- 142 are Anticipated by Russ.....	19
	1. Overview: Russ	19
	2. Claim Charts (140-142)	22
	3. Claim Charts (48-50, 57, 82-84, 91, 116-118, 125)	52
	B. Ground 2: Claims 48-50, 57, 82-84, 91, 116-118, 125, and 140- 142 are Obvious Over Russ.....	68

VIII. CONCLUSION.....	69
-----------------------	----

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Net MoneyIN, Inc. v VeriSign, Inc.</i> , 545 F.3d 1359 (Fed. Cir. 2008)	22
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	15
<i>Roku, Inc. v. VideoLabs, Inc.</i> , IPR2024-01024, paper 12 (PTAB Dec. 4, 2024)	1

Statutes

35 U.S.C. §112, ¶6	17
--------------------------	----

Other Authorities

37 C.F.R. §42.8	6
37 C.F.R. §42.100(b)	15
37 C.F.R. §42.104(a).....	9
37 C.F.R. §42.104(b)	9

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	RESERVED
1008	<i>VideoLabs, Inc. et al. v. Hisense Co. Ltd. et al.</i> , Case No. 2:24-cv-00904-JRG-RSP, Dkt. No. 1, Complaint Exhibit F – U.S. Patent No. 8,291,236 (“’236 Patent”) (Nov. 6, 2024)
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	OMITTED
1017	<i>VideoLabs, Inc. v. ASUSTeK Computer, Inc.</i> , Case No. 6:22-cv-00720 (W.D. Tex.), Dkt. No. 48, Plaintiff VideoLabs, Inc.’s Responsive Claim Construction Brief (Jun. 5, 2024)

I. INTRODUCTION

Hisense USA Corporation and Hisense Electronica Mexico S.A. de C.V. (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 (“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.

Indeed, the Board previously instituted *inter partes* review of the ’236 based on an identical petition. *Roku, Inc. v. VideoLabs, Inc.*, IPR2024-01024, paper 12 (PTAB Dec. 4, 2024). However, that proceeding was terminated because of settlement by the parties there. *Id.*, paper 16.

As to the ’236, 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

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

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 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).

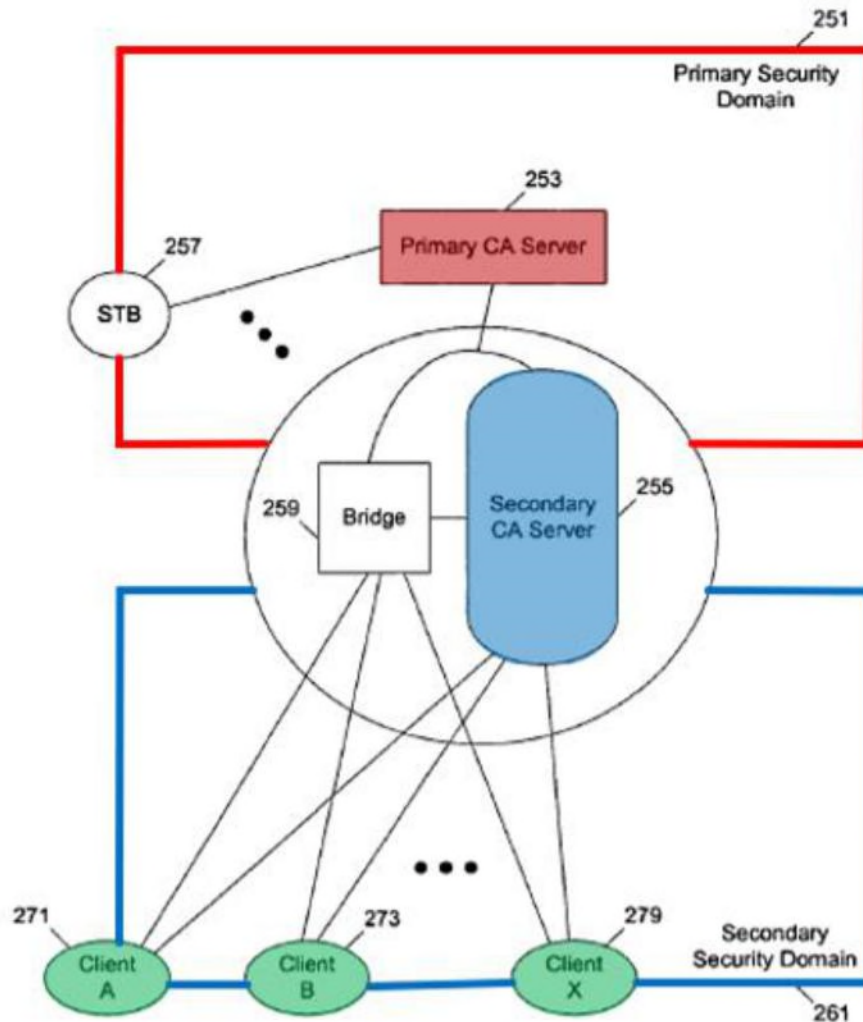


Fig. 2A

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**).

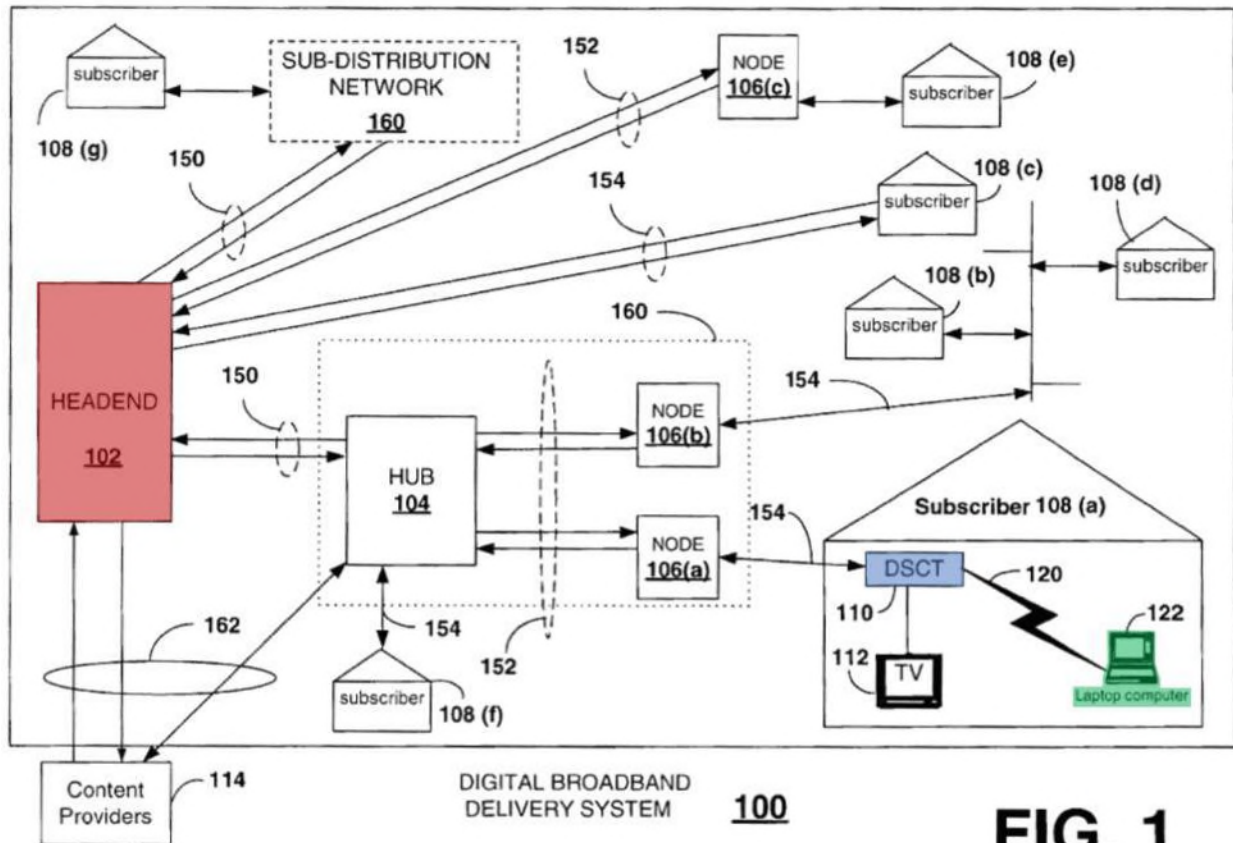


FIG. 1

Russ's system therefore bridges security systems, like the '236. Russ therefore anticipates the Claims of the '236. The USPTO did not consider Russ 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. Real Party-In-Interest

Petitioners Hisense USA Corporation and Hisense Electronica Mexico S.A. de C.V, and Hisense Co. Ltd. and its other related entities including: Hisense Visual Technology Co. Ltd. f/k/a Qingdao Hisense Electric Co. Ltd.; Hisense International

Co. Ltd.; Hisense International (Hong Kong) America Investments Co. Ltd.; Guiyang Hisense Electronics Co., Ltd.; Hisense International (HK) Co. Ltd.; Hisense Electronics Manufacturing Company of America Corporation; and Hisense Broadband Multimedia Technology Co., Ltd., are the real-parties 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. TCL Technology Corporation Group et al.</i>	2:25-cv-00161	E.D. Tex.	2025-02-10
<i>VideoLabs, Inc. v. Hisense et. al.</i>	2:24-cv-00904	E.D. Tex.	2024-11-06
<i>VideoLabs, Inc. v. ASUSTeK Computer Inc.</i>	6:22-cv-00720	W.D. Tex.	2022-06-30

Petitioner is also concurrently filing petitions for *inter partes* review with respect to other claims of the '236 and a petition for *inter partes* review of U.S. Patent No. 8,667,304, which claims to be a continuation of the '236, as identified below. Petitioner recommends assigning all petitions to the same panel and furthermore consolidating the proceedings directed to the '236.

Title	Patent	IPR No.
<i>Hisense Co. Ltd. et al. v. VideoLabs, Inc.</i>	8,291,236	IPR2025-00880
		IPR2025-00881
		IPR2025-00882

<i>Hisense Co. Ltd. et al. v. VideoLabs, Inc.</i>	8,667,304	IPR2025-00883
---	-----------	---------------

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

Lead Counsel	<p>Bas de Blank, Reg. No. 74,930</p> <p>Orrick, Herrington & Sutcliffe LLP 1000 Marsh Road Menlo Park, CA 94025 Email: M2BPTABDocket@orrick.com Phone: (650) 614-7400</p>
Backup Counsel	<p>Xiang Wang, Reg. No. 45,547</p> <p>Orrick, Herrington & Sutcliffe LLP 5701 China World, Tower A No.1 Jianguomenwai Avenue Beijing, 100004 People's Republic of China Email: XW0PTABDocket@orrick.com Phone: (949) 567-6700</p> <p>Richard Martinelli, Reg. No. 52,003</p> <p>Orrick, Herrington & Sutcliffe LLP 51 West 52nd Street New York, NY 10019 Email: RFMPTABDocket@orrick.com Phone: (212) 506-5000</p> <p>Thomas A. James, Reg. No. 74,109</p> <p>Orrick, Herrington & Sutcliffe LLP 353 N Clark Street, Suite 3600 Chicago, IL 60654 Email: PTABDocketT6J1@orrick.com Phone: (312) 924-9800</p>

Petitioner consents to electronic service of documents to the email addresses

of the counsel identified above.

III. REQUIREMENTS FOR IPR

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

Petitioner certifies the '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)

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	§102	48-50, 57, 82-84, 91, 116-118, 125, 140-142	Russ
2	§103	48-50, 57, 82-84, 91, 116-118, 125, 140-142	Russ

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 above, Fig. 2A below shows **secondary CA server 255** as a client of **primary CA server 253** (in primary security domain 251) and as a control information provider for **clients 271, 273, ..., 279** (in secondary security domain 261). '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.

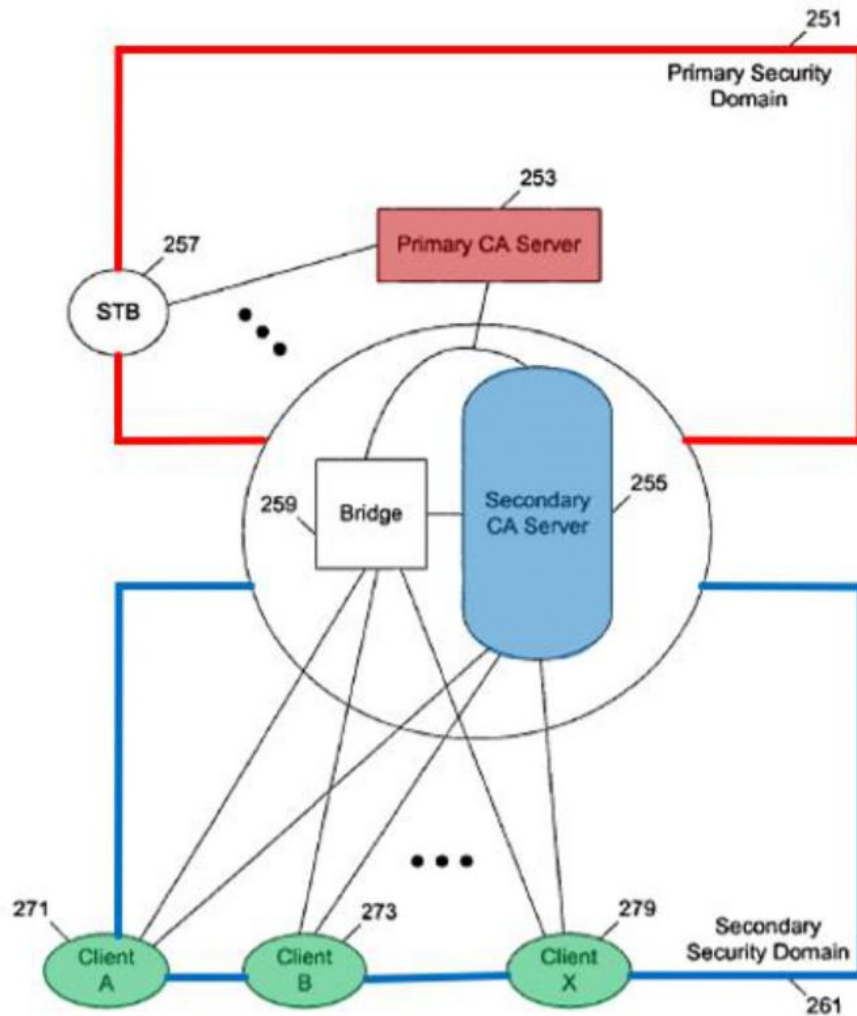


Fig. 2A

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.

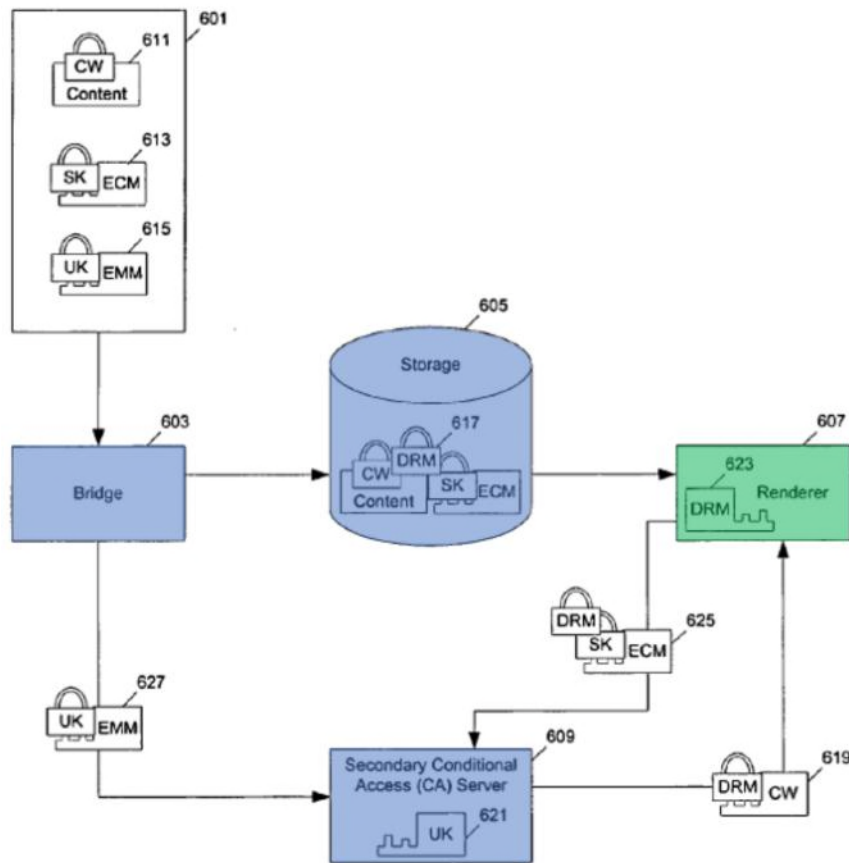


Fig. 11

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), which was originally filed with 146 claims, 15 being independent. EX1002 (“’236FH”), 1-129.

During prosecution, the Examiner repeatedly rejected the pending claims as being unpatentable over prior art applied alone or in combination, including U.S.

7,036,011 (“Grimes”), U.S. 7,302,058 (“Candelore”), U.S. 7,493,291 (“Simelius”), and U.S. 6,961,858 (“Fransdonk”). ’236FH, 296-324 (Rejection of 2009-04-01), 388-422 (Rejection of 2009-12-08), 506-541 (Rejection of 2012-01-03). Each subsequent rejection and application of the prior art was necessitated by continual amendments to the claims. ’236FH, 345-384 (Amendment of 2009-06-12), 434-480 (Amendment of 2010-03-02), 555-610 (Amendment of 2012-05-01). The Amendment of 2012-05-01, which preceded allowance of the claims, amended each of the independent claims, *inter alia*, to recite for the first time: “a first security domain,” “a second security domain,” client devices being of “the second conditional access server,” and “wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.” ’236FH, 556-599.

In the Notice of Allowance, the Examiner stated that “[n]owhere in the prior art is found, collectively ... ‘wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.’” ’236FH, 624. The ’236 issued 2012-10-16. ’236FH, 657. 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, 1017 (Fed. Cir. 2017).

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

Claims 48[a], 82[a.ii], 116[a], and 140[a.ii], recite “access controlled data that is in an access controlled format and that is at least partially derived from a security message.” 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 a security message.” 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	<div><div>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.</div><div>HWDRM: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked.</div></div>			
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, 20-21 (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 describing that the “access controlled format is... derived from a security message.” 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.

B. Means-plus-function terms

Construction of means-plus-function claim terms that invoke 35 U.S.C. §112, ¶6, requires identifying the claim terms and identifying corresponding structure disclosed in the specification that performs the identified functions and equivalents thereof.²

² Constructions of several *means* terms are disputed in related litigation not involving Petitioner. See EX1017, 19-33.

1. “means for receiving, at a secondary conditional access client”

“Means for receiving, at a secondary conditional access client” is recited at:

Claim	Text (functions of the means identified in bold)
116[a]	“means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data³ that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain ”

The '236 claims describe a “communication interface” to receive access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain. See claim 140; see also '236FH, 102 (claims as originally filed).

Thus, the structure in the specification linked to the claimed function, “means for receiving...,” includes a communication interface and statutory equivalents. Wasilewski, ¶¶53-55.

³ Every mapped structure in the grounds below receives access controlled data that is in accordance with the remainder of the limitation. No structure/function in the '236 derives an access controlled format from security messages. See §VI.A.

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, ¶¶1-171. The prior art renders the Claims unpatentable for reasons discussed below.

A. Ground 1: Claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 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:

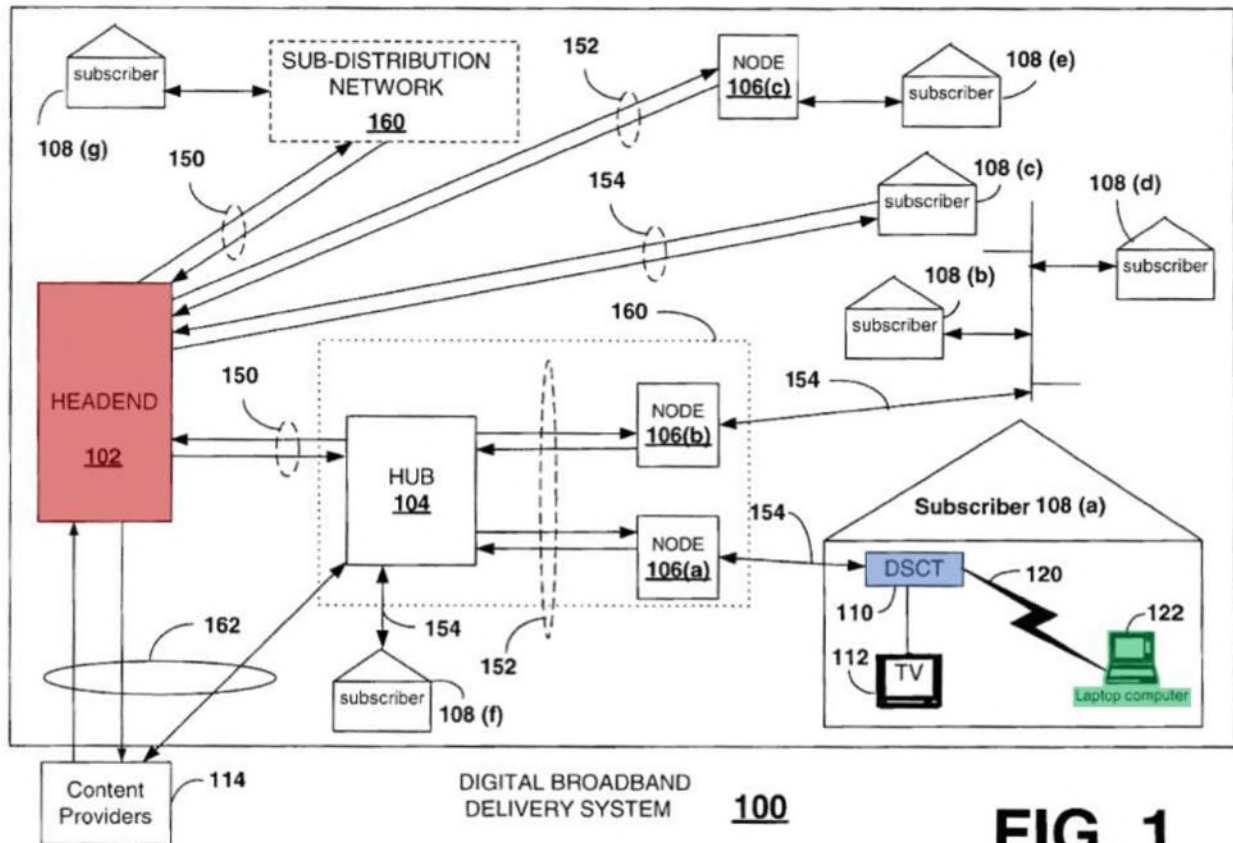


FIG. 1

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, ¶¶57-58.

DSCT 110 registers with **headend 102** and is granted entitlements to service instances before receiving and accessing those service instances. Russ, 7:56-8:3. Thus, **headend 102** implements conditional access authority (CAA) logic to

control access to DBDS 100 and, for example, grant entitlements to **DSCT 110** with control information and entitlement management messages (EMMs). Russ, 8:4-37, 10:48-50. **DSCT 110**, managing a local network at the subscriber location, 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, ¶¶59-62.

The specific protected communications by which **DSCT 110** and **client-receiver 122** communicate is determined dynamically when **client-receiver 122** joins **DSCT 110's** network and provides 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, ¶60.

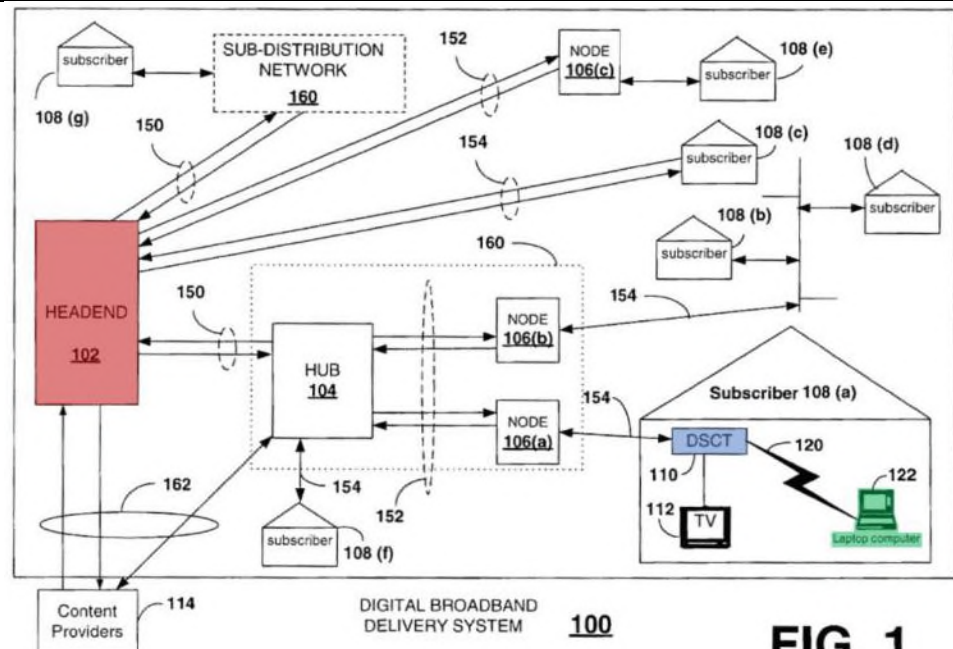
Because Russ discloses a first security server (**headend 102**) providing CA content (a service instance) and messages (EMMs and ECMs) to a CA server (**DSCT 110** receiving and processing the service instance, EMMs, and ECMs), and because the CA server (**DSCT 110**) communicates with clients (**client-receiver**

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 a secondary conditional access client, method to process media content, machine readable medium, and data processing system 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 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 of the '236. Wasilewski, ¶¶66-165.

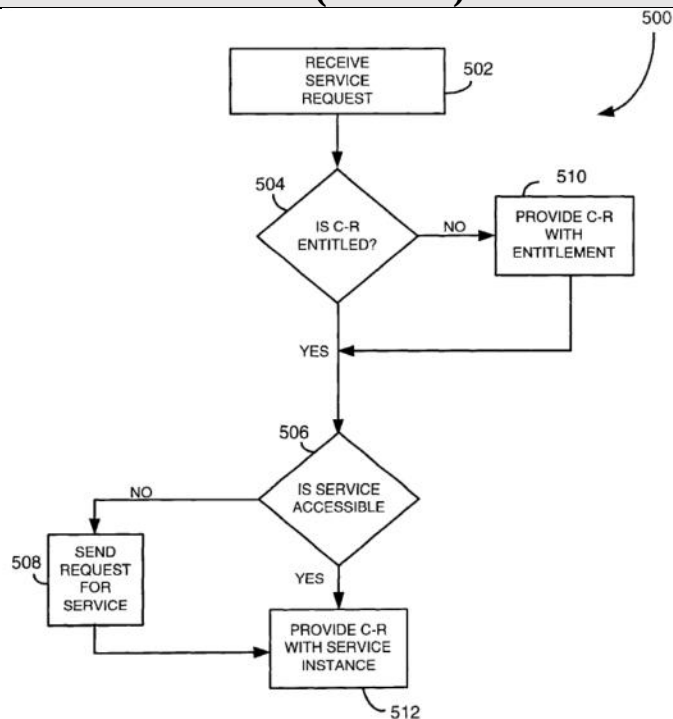
2. Claim Charts (140-142)

'236	Russ (EX1005)
<p>140[pre⁴]. A secondary conditional access client, comprising:</p>	<p>Russ discloses a secondary conditional access client (<i>e.g.</i>, client-receiver 122).</p> <p>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. Furthermore, DSCT 110 and client-receiver 122 operate together in a second security domain, as discussed for claims 140[a.ii] and 140[c.ii]-[c.iii] below. Client-receiver 122 is therefore a secondary conditional access client to the secondary conditional access server DSCT 110. Wasilewski, ¶¶66-71.</p> <p><i>E.g.,</i></p> <p>Regarding client-receiver 122 being a client to the secondary conditional access server DSCT 110:</p> <ul style="list-style-type: none"> • Fig. 1:

⁴ Regardless of whether the preambles (140[pre], 48[pre], 82[pre], 116[pre]) are limiting, the prior discloses it.



- 5:35-39 (“Referring to FIG. 1, a digital broadband distribution system (DBDS) 100 includes...a headend 102, ... a plurality of subscriber locations 108, and a plurality of digital subscriber communication terminals (DSCTs) 110.”)
- 8:49-51 (“The client-receiver 122 is in two-way communication with the DSCT 110 and receives information and service instances therefrom.”)
- Fig. 5:

**FIG. 5**

- 17:61-18:66 (“Referring to FIG. 5, steps 500 are implemented by processor 312 and the secure element 314. In step 502, the DSCT 110 receives a request from the client-receiver 122 for a service instance. The service instance is generally a user selected service instance such as a program selected by the user of the client-receiver 122....

In step 504, the secure element 312, which maintains a map of entitlements granted to the client-receiver, determines whether or not the client-receiver 122 is entitled to the requested service instance.

[...]

In step 510, the client-receiver 122 is provided with the entitlement for the selected service instance.... Typically, the secure element 314 generates an EMM, which includes the entitlement, and sends the entitlement to the client-

'236	Russ (EX1005)
	<p>receiver 122 via the communication link 120. In this embodiment, the DSCT 110 acts as an entitlement granting authority for the client-receiver 122. <u>The DSCT 110 has the authority and capacity to grant and delete entitlements to the client-receiver 122 for the service instance.</u></p> <p>[...]</p> <p><u>The secure element 314 of the DSCT 110 then processes the EMM and provides the entitlement to the client-receiver 122. In step 512, the selected service instance is provided to the client-receiver 122.”)</u></p> <ul style="list-style-type: none"> • See also 3:11-22, 4:21-39, 8:38-9:7, 19:7-42, 24:3-7, 24:37-38.
<p>140[a.i]. a communication interface to receive, from a conditional access server through a network connection,</p>	<p>Russ discloses a communication interface to receive, from a conditional access server (e.g., transceiver 902 receives entitlements, commands, and service instances from DSCT 110 via communication link 120) through a network connection (e.g., client-receiver 122 joins DSCT 110’s network and communicates via communication link 120).</p> <p>Russ discloses that client-receiver 122 includes a transceiver 902 for communicating with DSCT 110 and receiving, e.g., data, entitlements, authorizations. Russ, 25:34-42. 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, ¶¶72-75.</p> <p><i>E.g.,</i></p> <p>Regarding transceiver 902 of client-receiver 122:</p> <ul style="list-style-type: none"> • 25:34-42 (“<u>The client-receiver 122 includes a transceiver 902, a processor 904, a memory 906, a secure element 908, a user interface 910, a cryptographic device 912 and an output port/interface 916. The transceiver 902 receives information such as data, entitlements, authorizations, commands and service instances from the DSCT 110 via communication link 120.</u> The transceiver 902 is adapted to transmit information to the DSCT 110 via communication

link 120.”)

- Fig. 9

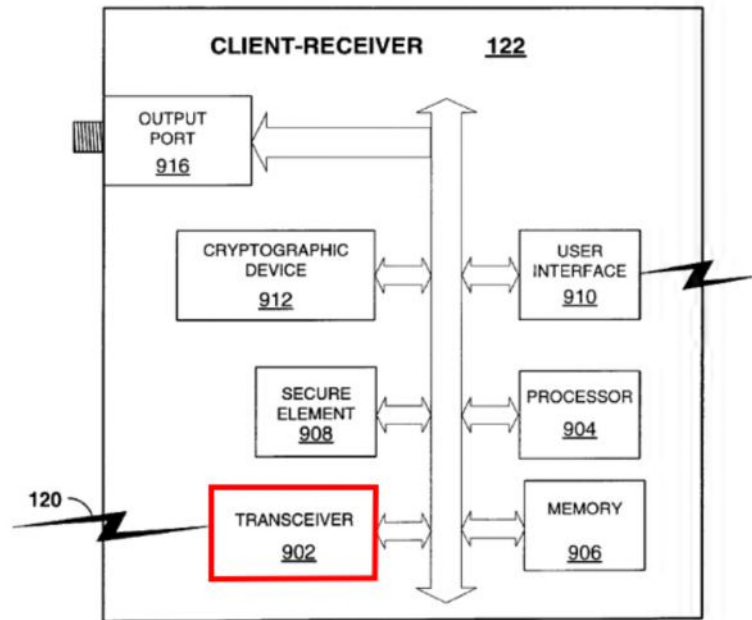


FIG. 9

Regarding receiving information from **DSCT 110**:

- Fig. 1

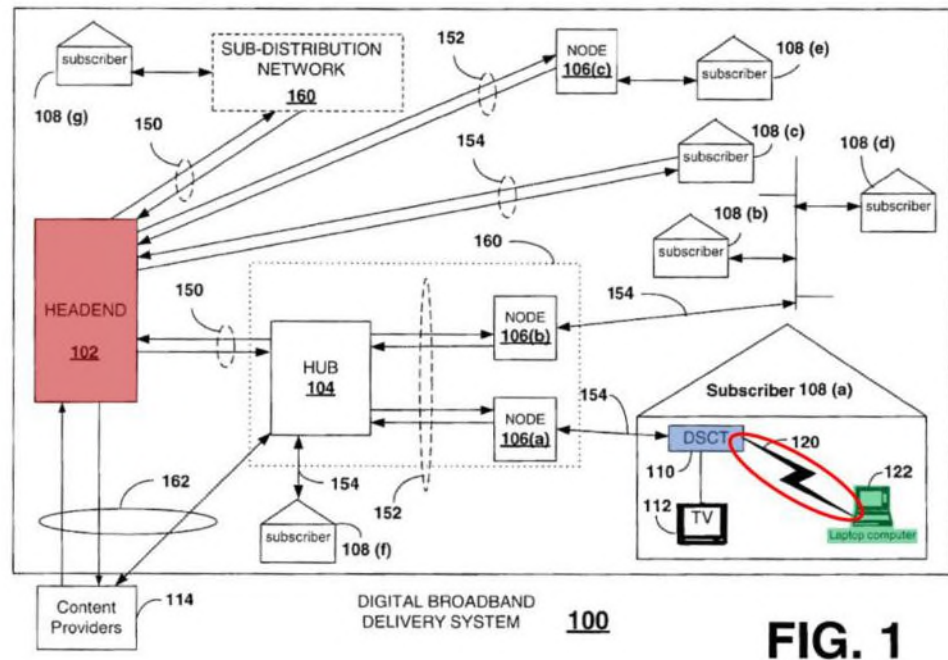


FIG. 1

- 8:38-48 (“The DSCT 110 is preferably in communication with client-receiver 122 via communication link 120. In the preferred embodiment, the communication link 120 is wireless such as, but not limited to, Institute for Electronics and Electrical Engineers (IEEE) standards 802.11a, 802.11b, 802.11g, HiperLAN/2, HomeRF 2, Bluetooth 2, and 802.15.3. In alternative embodiments, the DSCT 110 is in communication with multiple client-receivers via one or more communication links, such as, but not limited to, twisted-wire or Ethernet, telephone line, electrical power line and coaxial cable.”)
- 9:8-20 (“In the preferred embodiment, the local network at the subscriber location 108 is self-aware. When a new client-receiver 122 is brought into the local network, the client-receiver 122 discovers the network and communicates with the DSCT 110. In one embodiment, the client-receiver 122 and the DSCT 110 communicate via a standard such as Open Server Gateway interface (OSGi). Other non-limiting embodiments include communicating via Universal Plug and Play (UPnP), Home Audio Video Interoperability (HAVi) and Jini. The choice of a communication protocol is a matter of

'236	Russ (EX1005)
	implementation and factors for choosing the communication protocol include the type of communication link coupling the DSCT 110 to the client-receiver 122 and the type of client-receiver 122.”)
<p>140[a.ii]. [communication interface to receive] access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain; and</p>	<p>Russ discloses the communication interface to receive access controlled data that is in an access controlled format (e.g., DSCT 110 transmits EMMs and service instances to client-receiver 122 using a dynamically determined encryption scheme) and that is at least partially derived from a security message of a primary security system (e.g., DSCT 110 receives entitlement management messages (EMMs) of/from headend 102; EMMs include entitlement and key information for service instances; DSCT 110 receives entitlements in the EMM, then provides entitlements to client-receiver 122) in a first security domain (e.g., headend 102 implements conditional access authority (CAA) logic to control access to service instances for a plurality of DSCTs 110; headend 102 and DSCT 110 exchange public keys to establish and conduct secure communications with each other), the secondary conditional access client being in a second security domain (e.g., 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). Wasilewski, ¶¶76-84.</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, ¶81.</p> <p>As discussed with respect to claim 140[pre] above, client-receiver 122 is a conditional access client to DSCT 110, which serves service instances to client-receiver 122 (and to other</p>

'236	Russ (EX1005)
	<p>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, 20:12-24. 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, ¶¶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, 14:36-42; see '236 claim 101 (security messages include EMMs). Entitlements received by client-receiver 122 are, for example, based on the EMMs received at DSCT 110 and are thus at least partially derived from the security message. 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 client-receiver 122. Russ, 8:8-34, 15:46-52. Therefore, service instances are also partially derived from the security messages. Wasilewski, ¶79.</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

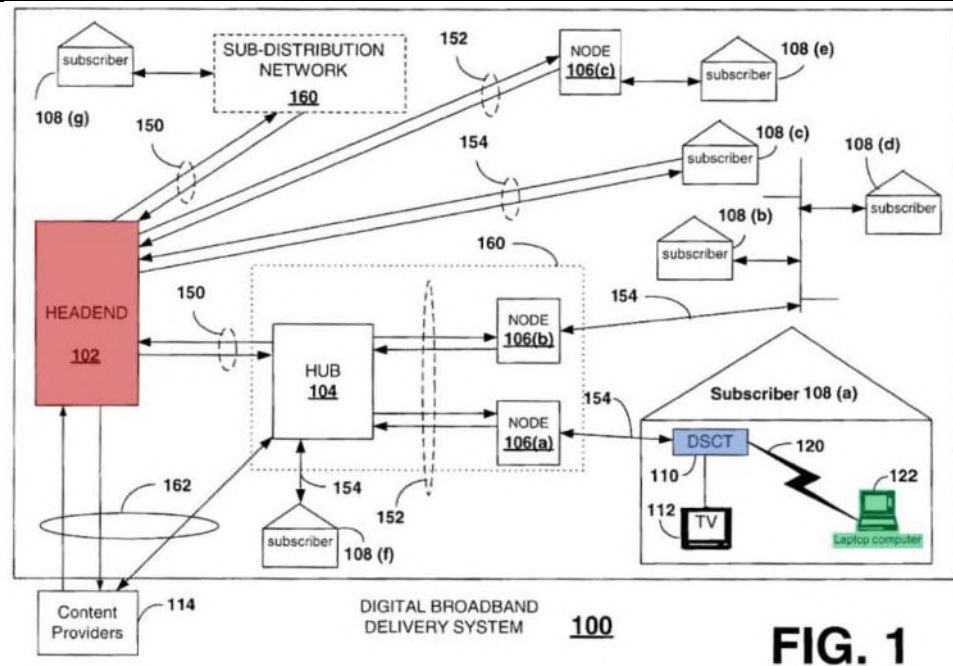


FIG. 1

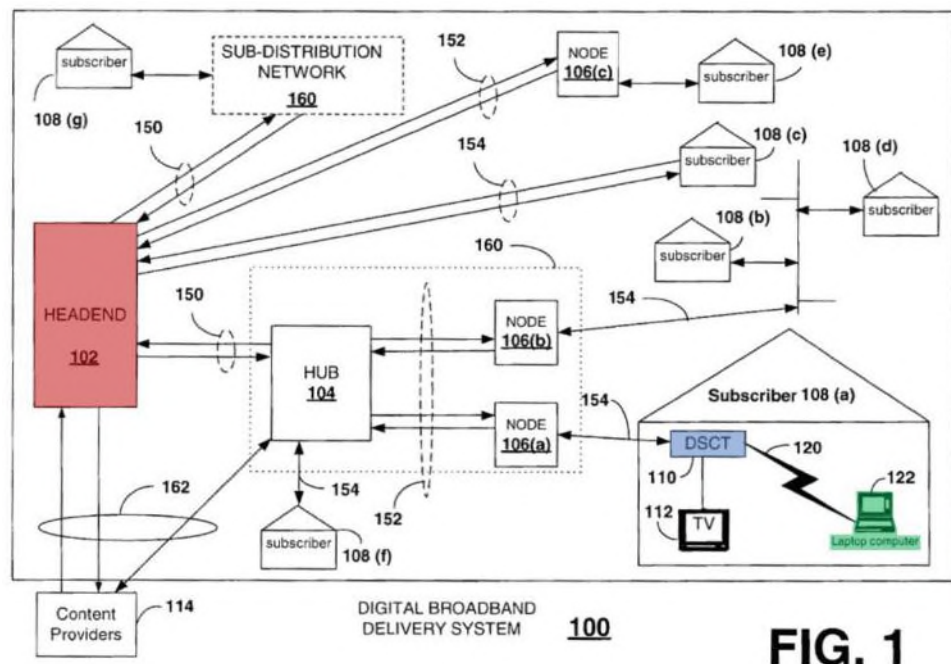
- 6:62-7:6 (“Secure communication between the headend 102 and the DSCTs 110 is preferably accomplished using pairs of asymmetrical keys known to those skilled in the art, such as Rivest, Shamir, & Adleman (RSA) public key encryption technology. [...] The headend 102 and the DSCT 110 can securely communicate after they have exchanged public keys.”)
- 7:56-58 (“Before the DSCT 110 receives and accesses service instances from the headend 102, the DSCT 110 is registered with the headend 102 and entitled to the service instances.”)
- 8:8-22 (“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. For the purposes of this disclosure, a secure message includes, as a non-limiting example, a message that has been digitally signed by the sender so that the recipient can verify the source of the message and verify that the content of the received

message was not tampered with nor corrupted in transmission. The content of a secure message may be encrypted when the sender wants to make the content private or the content can be transmitted without encryption.”)

- 10:48-65 (“The CAA 234 is used by the access controlling authority to enable DSCTs 110 to receive entitlements for service instances. The CAA 234 receives EMM templates from the EMM generator 238 and uses the EMM template to create an EMM. To create an EMM, the CAA 234 includes a message content and an authentication token in the EMM template.... In the preferred embodiment, the recipient, i.e., the DSCT 110, implicitly trusts any EMM that has an authentication token from the CAA 234 because the CAA 234 signs the hash digest with the private key that corresponds to one of the trusted public keys stored in the DSCT 110.”)

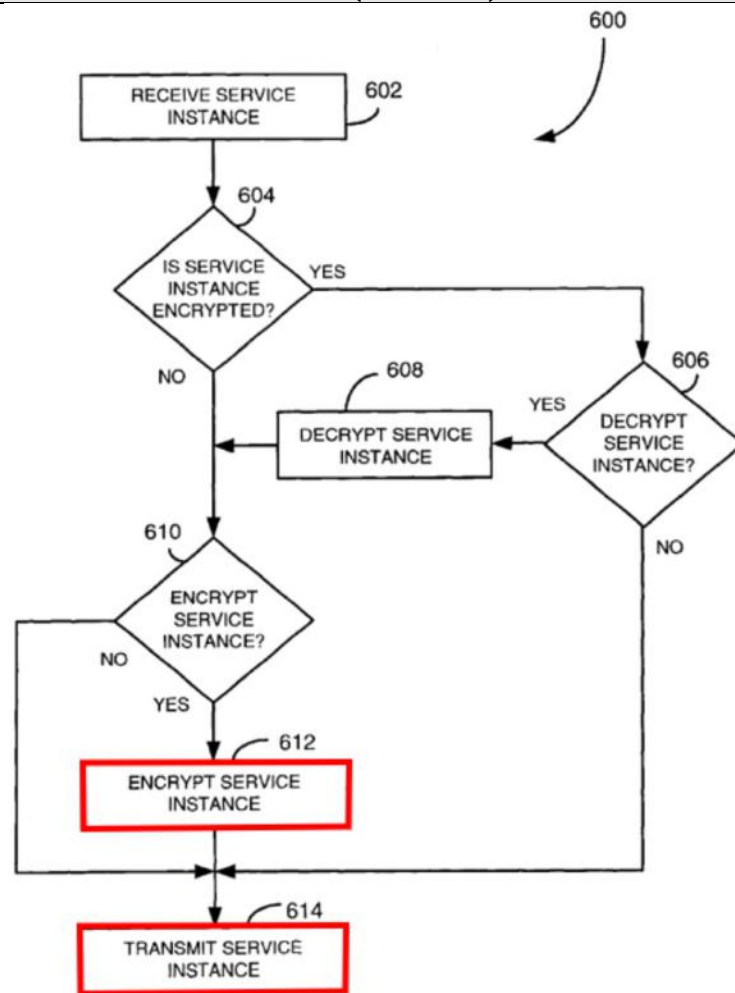
Regarding **DSCT 110** and **client-receiver 122** being in a second security domain and communicating information in an access controlled format:

- Fig. 1



'236	Russ (EX1005)
	<ul style="list-style-type: none"> <li data-bbox="505 245 1430 1052">16:64-17:14 (“The memory 310 includes logic for <u>dynamic encryption scheme determination</u>. <u>Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication.</u> <u>The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium.</u> For example, when the client-receiver 122 is a laptop, the encryption scheme may be different from when the client-receiver 122 is a PDA or set top. Non-limiting examples of dynamic encryption scheme determination logic include, but are not limited to, secure sockets layer (SSL) protocol, Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol. These protocols and other dynamic encryption scheme determination logic known to those skilled in the art are intended to be within the scope of the invention.”) <li data-bbox="505 1073 643 1115">Fig. 4 <div data-bbox="800 1127 1118 1650" data-label="Diagram"> <pre> graph TD 402[RECEIVE CLIENT-RECEIVER IDENTIFICATION MESSAGE] --> 404[DETERMINE CLIENT-RECEIVER CLASSIFICATION] 404 --> 406[DYNAMIC DETERMINATION OF ENCRYPTION SCHEME] </pre> </div> <p data-bbox="881 1822 1062 1881" style="text-align: center;">FIG. 4</p>

'236	Russ (EX1005)
	<ul style="list-style-type: none"> <li data-bbox="505 247 1435 621">• 17:15-34 (“Referring now to FIG. 4, the steps 400 are implemented for establishing private communication between the DSCT 110 and the client-receiver 122. In step 402, the DSCT 110 receives a client-receiver identification message from the client-receiver. The message is sent to the DSCT 110 when the client-receiver 122 discovers the local network maintained by the DSCT 110. The message includes device information such as hardware information about the client-receiver 122. In step 404, the processor 312 uses tables stored in memory 310 and the received client-receiver identification message to determine a classification for the client-receiver 122. <u>The processor 312 in negotiating an encryption scheme with the client-receiver 122 uses the classification of the client-receiver 122.</u> <u>In step 406, the processor 312 implements logic for negotiating an encryption scheme for the client-receiver 122. In the preferred embodiment, the encryption scheme is determined dynamically, when the client-receiver 122 is coupled to the local area network.</u>”) <li data-bbox="505 1150 643 1182">• Fig. 6

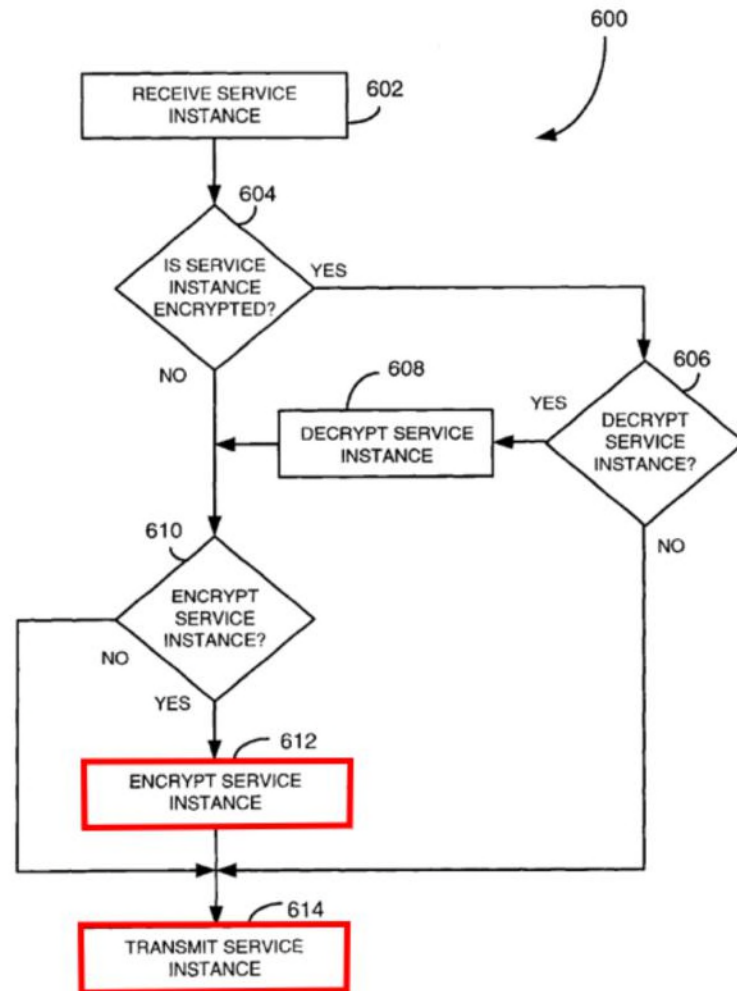
**FIG. 6**

- 20:12-24 (“When the processor 312 determines to encrypt the service instance, then in step 612, the service instance is provided to the cryptographic device 318. The cryptographic device 318 encrypts the service instance using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122. Typically, the secure element 314 provides the cryptographic device 318 with the encryption keys used by the cryptographic device 318 to encrypt the service instance.

[...] In step 614, the client-receiver interface 320 transmits

'236	Russ (EX1005)
	<p>the service instance to the client-receiver 122.”)</p> <ul style="list-style-type: none"> 20:25-53 (“Referring to FIG. 7, the secure element 314 <u>includes</u> a processor 702 and a memory 704. The memory 704 is accessible only to the processor 702 and it includes entitlements 706, <u>secrets 708</u>, and keys 710. [...] The secrets 708 are secrets that are shared between the DSCT 110 and the client-receiver 122. In the preferred embodiment, the secrets 708 are used for, among other things, encrypting service instances provided to the client-receiver 122, generating authentication tokens for messages transmitted to the client-receiver 122 and authenticating messages from the client-receiver 122.”) <p>Regarding DSCT 110 receiving 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 only if the EMM is authenticated as having come from the conditional access authority. <u>Among other things, the conditional access authority uses EMMs to instruct the DSCT 110 to allocate a portion of its memory for entitlement information related to a service instance provided by an entitlement agent and to provide the DSCT 110 with the public key for an entitlement agent.</u>”) 14:36-42 (“<u>In the preferred embodiment, the transceiver 308 receives out-of-band communication 258 from input port 302. The out-of-band communication data includes among other things system tables and messages including secure messages such as EMMs. EMMs are sent to the secure element 314 for processing and the system tables are stored in memory 310.</u>”) Regarding deriving access controlled data from security messages and transmitting access controlled data to client-receiver 122: 8:8-22 (<i>see above</i>)

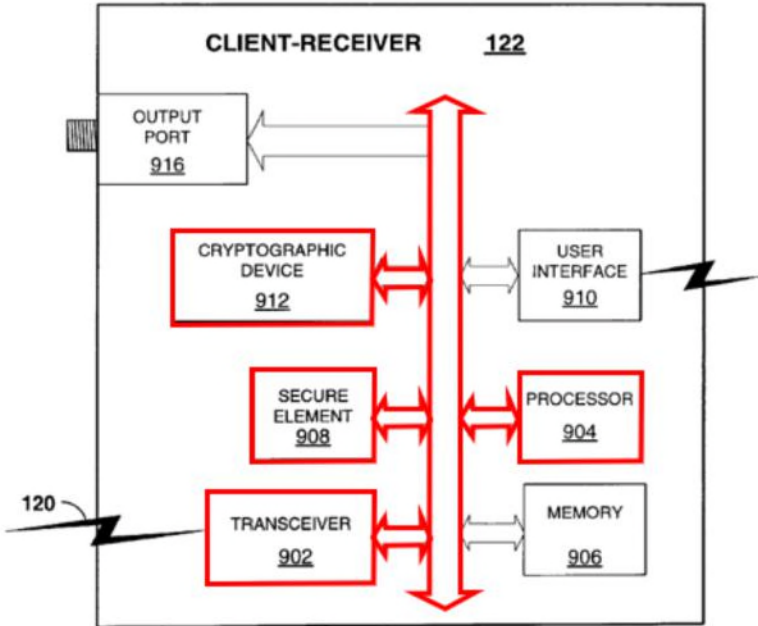
'236	Russ (EX1005)
	<ul style="list-style-type: none"> • 8:25-34 (<i>see above</i>) • 15:46-52 (“When the DSCT 110 is entitled to the selected service instance.... The cryptographic device 318 decrypts the selected service instance using the control word from the secure element 314 and the decrypted service instance is sent to the output port 322.”) • 18:52-65 (“In one preferred embodiment, the secure 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

**FIG. 6**

- 20:12-24 (see above)
- 21:11-21 (“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 authenticates messages from the client-receiver 122, and generates secure messages for the client-receiver 122. [...] If the EMMs are for the DSCT 110 and are authenticated by the AEMM 720, the AEMM 720 responds to the EMMs and implements them.”)
- 21:22-65 (“Referring now to FIG. 8A, an entitlement

'236	Russ (EX1005)
	<p>management message 800 includes an address field 802, message content 804 and an authentication token 806. <u>EMM 800 is a typical EMM used for securely transmitting information...</u> between the headend 102 and the DSCT 110, between the headend 102 and the client-receiver 122, and the <u>between the DSCT 110 and the client-receiver 122.</u> The EMM 800 is an exemplary secure message.</p> <p>[...]</p> <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 in the DBDS 100 and between the DSCT 110 and the client-receiver 122.”)</u></p> <ul style="list-style-type: none"> • 24:1-24 (“In the preferred embodiment, the AEMM 720 includes logic for granting entitlements to the client-receiver 122 for service instances. When the AEMM 720 receives a request from the client-receiver 122 for a service instance, the AEMM 720 determines whether the client-receiver 122 is currently entitled to the service instance by checking the entitlements 706. <u>If the client-receiver 122 is not entitled, the AEMM 720 determines whether to entitle the client-receiver 122. 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.</u> In other words, the array element of elements 706 associated with the service instance would be changed from NO to YES or from 0 to 1. The AEMM 720 can also delete an entitlement for the client-receiver 122 to a service instance by changing the array element that is associated with the service instance. In the preferred embodiment, the client-receiver 122 includes an entitlement map that it uses for

'236	Russ (EX1005)
	<p>accessing received service instances. 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. The client-receiver 122 receives the EMM and processes it, thereby updating its entitlements.”)</p> <p>See also:</p> <ul style="list-style-type: none"> • 1:45-2:10, 3:17-20, 7:7-20, 10:39-65, 11:37-61, 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—which conflates the grammatical clauses in the claim language, is not a reasonable reading of the claim language, and which furthermore has no support in the '236 specification (<i>see</i> §VI.A above)—Russ discloses the access controlled format partially derived from the security messages (<i>e.g.</i>, headend 102 transmits an EMM to DSCT 110 dictating the encryption scheme for communications with client-receiver 122). Wasilewski, ¶83.</p> <ul style="list-style-type: none"> • 25:17-25 (“<u>The system controller 232 can also send an EMM to the DSCT 110 instructing the processor 312 to no longer determine the encryption scheme for the client-receiver 122. In that case, the headend 102 determines the encryption scheme used to communicate information between the DSCT 110 and the client-receiver 122. The headend uses information related to the hardware and software of the client-receiver 122 and the type of communication link 120 between the DSCT 110 and the client-receiver 122.</u>”) • <i>See also</i> 16:31-63, 19:7-27.
<p>140[b]. a processor coupled to the communication interface, the processor to</p>	<p>Russ discloses a processor coupled to the communication interface (<i>e.g.</i>, processor 904, secure element 908, and cryptographic device 912 are coupled to transceiver 902), the processor to process the access controlled data (<i>e.g.</i>, secure element 908 processes received EMMs).</p> <p>Russ discloses that client-receiver 122 includes processor 904,</p>

'236	Russ (EX1005)
<p>process the access controlled data,</p>	<p>cryptographic device 912, and secure element 908, which includes a processor, which are coupled to transceiver 902. Russ, Fig. 9, 25:34-37, 26:60-61. Secure element 908 processes received EMMs. Russ, 26:16-28. Cryptographic device 912 and secure element 908 together process received service instances. Russ, 26:61-64. Alternatively, cryptographic device 912 and processor 904 together process received service instances. Russ, 27:1-7. Wasilewski, ¶¶85-88.</p> <p><i>E.g.,</i></p> <ul style="list-style-type: none"> Fig. 9  <p style="text-align: center;">FIG. 9</p> <ul style="list-style-type: none"> 26:16-28 (“<u>In the preferred embodiment, the secure element 908 includes a processor (not shown) and a memory (not shown) that are included in tamper resistant packaging. Among other things, the secure element 908 generates secure messages; processes received EMMs, and generates control words for the cryptographic device 912.</u>”)

'236	Russ (EX1005)
	<p>The secure element 908 includes entitlements granted to the client-receiver 122, secrets for authenticating messages and generating control words, and keys such as a private key-public key pair of the client receiver 122 and other public keys. The other public keys include trusted public keys, the public key of the conditional access authority 234 and the public key of the DSCT 110.”)</p> <ul style="list-style-type: none"> • 26:60-64 (“[T]he transceiver 902 sends the service instance to the cryptographic device 912 for decryption. The cryptographic device 912 decrypts the service instance using control words provided by the secure element 908 and sends the decrypted service instance to the output port 916.”) • 27:1-7 (“Those skilled in the art will recognize that the client-receiver 122 can include more or fewer modules than described hereinabove. For example, in a non-limiting alternative embodiment, the client-receiver 122 does not include a secure element 908. The processor 904 provides the cryptographic device 912 with the control words for decrypting received service instances.”) • See also 26:49-51.
<p>140[c.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</p>	<p>Russ discloses that the primary security system authenticates the conditional access server as one of clients of the first primary security system through a first authentication process using a first root of trust (e.g., headend 102 authenticates DSCTs 110 when they connect to the DBDS)</p> <p>Russ discloses that headend 102 authenticates a DSCT 110 by verifying that DSCT 110’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 110; DBDS 100 registers DSCT 110 as a client to receive service instances. Russ, 7:21-8:3, 10:39-47. Wasilewski, ¶¶90-93.</p> <p>“Root of trust” is not explicitly defined in the ’236, but in context, a POSA would have recognized it as at least including</p>

'236	Russ (EX1005)
	<p>hardware, software, and/or firmware-based systems for establishing trustworthy identities of components or entities, as in Russ. Wasilewski, ¶92.</p> <p><i>E.g.,</i></p> <ul style="list-style-type: none"> 7:21-39 (“<u>In the preferred embodiment, when the DSCT 110 is manufactured it is assigned a serial number, and it is provided with its own private key-public key pair and with a public key of an access controlling authority. The keys are provided to the DSCT 110 in a secure manner and stored in a protected memory in the DSCT 110. The manufacturer of the DSCT maintains a database that includes the public keys and the serial numbers of each of the DSCTs 110 that the manufacturer produces. Each DSCT 110 in the DBDS 100 has a unique serial number, and the serial number, which can be the MAC address of the DSCT 110, is used for addressing messages to the DSCT 110. The manufacturer provides a copy of the public key and the serial number of each DSCT 110 in the DBDS 100 to the operator of the DBDS 100. In that case, the manufacturer is a key certification authority that certifies to the operator of the DBDS 100 that a given public key belongs to a specific DSCT 110. The operator of the DBDS 100 maintains its database of public keys and serial numbers of each DSCT 110 in the DBDS 100.</u>”) 7:40-55 (“<u>In the preferred embodiment, the DSCT 110 is provided with multiple public keys during its manufacture. Because these keys were given to the DSCT 110 during its manufacture in a secure fashion, the DSCT 110 implicitly trusts these keys. The DSCT 110 trusts any message that is signed by a private key corresponding to one of these trusted public keys. At least one of the trusted public keys can be replaced by a different public key, which then becomes a trusted public key. To replace a trusted key the DSCT 110 receives at least two messages with a new trusted public key included therein. A private key corresponding to one of the trusted public keys that are not being replaced signs each of the messages. The DSCT 110</u>

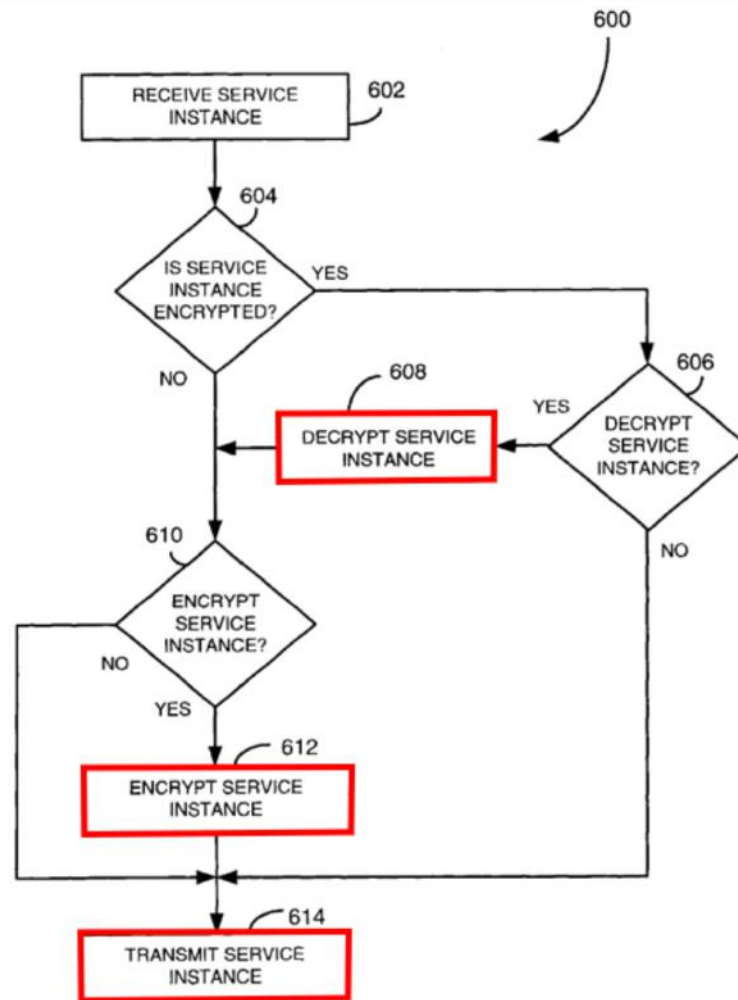
'236	Russ (EX1005)
	<p>uses its trusted public keys to verify that the messages were signed by one of the corresponding private keys. The DSCT 110 only replaces one of its trusted public keys when the message is verified.”)</p> <ul style="list-style-type: none"> • 7:56-8:3 (“<u>Before the DSCT 110 receives and accesses service instances from the headend 102, the DSCT 110 is registered with the headend 102 and entitled to the service instances. When the DSCT 110 is connected to the DBDS 100, it sends a message, which includes the serial number of the DSCT 110, to the headend 102. The operator of the DBDS 100 compares the serial number of the DSCT 110 against its database and registers the DSCT 110 if the database includes the serial number of the DSCT 110. Generally, the operator of the DBDS 100 replaces one of the trusted public keys of the DSCT 110 with its own trusted public key. This is accomplished by having the manufacturer of the DSCT 110 digitally sign two messages, which include the new trusted public key, for the DSCT 110 and then sending the two messages to the DSCT 110.</u>”) • 10:39-47 (“The control system 232 includes <u>database 240 and logic for conditional access authority (CAA) 234, entitlement generator 236 and EMM generator 238. Database 240 includes, among other things, the serial numbers and public keys of the DSCTs 110 of DBDS 100. The EMM generator 238 uses database 240 to generate individually addressable EMM templates. The EMM generator 238 can also generate EMM templates for multiple DSCTs 110 and/or global EMM templates.</u>”) • <i>See also 8:4-11.</i>
<p>140[c.ii]. the conditional access server authenticates clients of the conditional access server</p>	<p>Russ discloses that the conditional access server authenticates clients of the conditional access server through a second authentication process (e.g., 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</p>

'236	Russ (EX1005)
<p>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</p>	<p>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 claim 140[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. See discussion of claim 140[a.ii] above. 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. See, <i>e.g.</i>, EX1010 (US 2002/0025042), [0009] (describing an authentication and key exchange procedure between transmitting and receiving devices under DTCP); EX1011 (US 2005/0027984), [0053] and [0107] (describing device identification numbers embedded in a device certificate issued by a licensing institution such as the DTLA), [0139]-[0143] and Fig. 17 (describing a "DTCP communication sequence" including an authentication and key exchange prior to transmission of content). 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, ¶¶94-99.</p> <p><i>E.g.</i>,</p> <ul style="list-style-type: none"> • 16:64-17:14 ("The memory 310 includes logic for dynamic encryption scheme determination. Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication. <u>The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by</u>

'236	Russ (EX1005)
	<p><u>considering factors such as the device type of the client-receiver 122 and the communication medium. For example, when the client-receiver 122 is a laptop, the encryption scheme may be different from when the client-receiver 122 is a PDA or set top. Non-limiting examples of dynamic encryption scheme determination logic include, but are not limited to, secure sockets layer (SSL) protocol, Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol. <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>”)</u></p>
<p>140[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.</p>	<p>Russ discloses that the conditional access server is configured to substitute the first security domain with the second security domain (e.g., 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 (e.g., client-receiver 122 and other client-receivers 122 are under the second root of trust established with DSCT 110, see discussion of claim 140[c.ii]).</p> <p>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 service instance may be encrypted/decrypted by a multi-session key and CA control words (see Russ, 11:37-61, 13:12-34), while the re-encrypted service instance is protected by DTCP encryption between DSCT 110 and client-receiver 122 (see discussion of claim 140[a.ii, c.ii] above). DSCT 110 therefore substitutes the first security domain using CA with the second security domain using DTCP. Wasilewski, ¶¶100-105.</p> <p><i>E.g.,</i></p> <p>Regarding the first security domain including headend 102 and DSCT 110:</p>

'236	Russ (EX1005)
	<ul style="list-style-type: none"> <li data-bbox="505 243 1437 709">• 11:37-46 (“The entitlement generator 236 generates encryption information and the entitlements of the DSCTs for the service instances. The entitlement generator 236 provides the encryption information to the multi-transport stream transceiver 228, which generates control words therefrom for encrypting the service instances. <u>In the preferred embodiment, the encryption information is a multi-session key (MSK), which has a relatively long life, such as days, weeks, or months. The MSK is transmitted to the DSCTs 110 in EMMs created by the entitlement generator 236.</u>”) <li data-bbox="505 730 1437 1108">• 13:12-34 (“<u>The multi-transport stream transmitter/receiver 228 uses the MSK from the control system 232 to encrypt service instances.</u> The multi-transport stream transmitter/receiver 228 includes a counter that produces a numerical value every couple of seconds or so and an encryptor. <u>The encryptor uses the MSK to encrypt the counter value to produce a control word. The control word is used by the encryptor as a key for encrypting a portion of the service instance.</u> The multi-transport stream transmitter receiver 228 includes the counter value in an entitlement control message (ECM), which is multiplexed into the output transport stream 242. [...] <u>Only DSCTs that have the MSK will be able to encrypt the counter value of the ECM to generate the control word that decrypts the service instance.</u>”) <p data-bbox="487 1444 1380 1528">Regarding the second security domain including DSCT 110 and client-receiver 122:</p> <ul style="list-style-type: none"> <li data-bbox="505 1549 1437 1881">• 16:64-17:14 (“The memory 310 includes logic for dynamic encryption scheme determination. <u>Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium. For example,</u>

'236	Russ (EX1005)
	<p>when the client-receiver 122 is a laptop, the encryption scheme may be different from when the client-receiver 122 is a PDA or set top. Non-limiting examples of dynamic encryption scheme determination logic include, but are not limited to, secure sockets layer (SSL) protocol, Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol. These protocols and other dynamic encryption scheme determination logic known to those skilled in the art are intended to be within the scope of the invention.”)</p> <ul style="list-style-type: none"> • 17:15-34 (see claim 140[a.ii]) <p>Regarding DSCT 110 substituting the first security domain for the second security domain:</p> <ul style="list-style-type: none"> • 15:46-52 (“When the DSCT 110 is entitled to the selected service instance, the secure element 314 provides the cryptographic device 318 with the control word used for decrypting the selected service instance. <u>The cryptographic device 318 decrypts the selected service instance using the control word from the secure element 314 and the decrypted service instance is sent to the output port 322.</u>”) • Fig. 6

**FIG. 6**

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

On the other hand, when the processor 312 determines to decrypt the service instance, the processor 312 instructs the tuner to send the service instance to the cryptographic device 318. In step 608, the cryptographic device 318 decrypts to the service instance using the control word(s) provided by the secure element 314.

In step 610, the processor 312 determines an encryption scheme for the selected service instance. [...]

'236	Russ (EX1005)
	<p><u>When the processor 312 determines to encrypt the service instance, then in step 612, the service instance is provided to the cryptographic device 318. The cryptographic device 318 encrypts the service instance using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122. Typically, the secure element 314 provides the cryptographic device 318 with the encryption keys used by the cryptographic device 318 to encrypt the service instance.”)</u></p> <p>See also:</p> <ul style="list-style-type: none"> • 8:49-9:7, 23:47-67
<p>141[pre]. The client of claim 140,</p>	<p>See claim 140.</p>
<p>141[a]. wherein the security message is an entitlement management message; and</p>	<p>Russ discloses that the security message is an entitlement management messages (<i>e.g.</i>, DSCT 110 receives an EMM).</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 claim 140[a.ii] above. Wasilewski, ¶¶107-109.</p>
<p>141[b]. wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.</p>	<p>Russ discloses that the secondary conditional access client does not have a user key representing a subscriber of the primary security system (<i>e.g.</i>, client-receiver 122 generates control words using secrets shared with DSCT 110 and therefore has a user key representing a subscriber of DSCT 110; client-receiver 122 does not have a user key as a subscriber of headend 102).</p> <p>Russ discloses that secrets are shared between DSCT 110 and client-receiver 122 for client-receiver 122 to, <i>e.g.</i>, generate control words to decrypt service instances. Russ, 20:47-53, 26:18-25. Client-receiver 122 does not have or require similar shared secrets with headend 102. <i>See also</i> Russ, 8:49-9:7 (DSCT 110 decrypts information from headend 102 and re-encrypts them for client-receiver 122. Wasilewski, ¶¶110-113. <i>E.g.</i>,</p>

'236	Russ (EX1005)
	<p>Regarding client-receiver 122 sharing secrets with DSCT 110 but not with headend 102:</p> <ul style="list-style-type: none"> • 20:47-53 (“<u>The secrets 708 are secrets that are shared between the DSCT 110 and the client-receiver 122. In the preferred embodiment, the secrets 708 are used for, among other things, encrypting service instances provided to the client-receiver 122, generating authentication tokens for messages transmitted to the client-receiver 122 and authenticating messages from the client-receiver 122.</u>”) • 26:18-25 (“Among other things, the secure element 908 generates secure messages; processes received EMMs, and generates control words for the cryptographic device 912. <u>The secure element 908 includes entitlements granted to the client-receiver 122, secrets for authenticating messages and generating control words, and keys such as a private key-public key pair of the client receiver 122 and other public keys.</u>”) <p>See also:</p> <ul style="list-style-type: none"> • 8:49-9:7
<p>142. The client of claim 140, wherein the access controlled format protects access to data using a digital rights management system.</p>	<p>Russ discloses that the access controlled data is protected using a digital rights management system (<i>e.g.</i>, communications between DSCT 110 and client-receiver 122 are protected by a DTCP scheme—a DRM system).</p> <p>Russ discloses that the access controlled data transmitted from DSCT 110 to client-receiver 122 are protected by DTCP. Russ, 16:64-17:14; see discussion of claim 140[c.ii] above. 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, ¶¶114-116.</p>

3. Claim Charts (48-50, 57, 82-84, 91, 116-118, 125)

Independent claims 48, 82, 116, and their dependent claims are respectively directed to method steps, program instructions for performing method steps, and data processing system components with limitations that are substantially similar to the functions, steps, and related structures in independent client claim 140 and its dependent claims. Claims 48-50, 57, 82-84, 91, 116-118, and 125 are therefore disclosed for the same reasons identified above and as shown in the chart below. Wasilewski, ¶¶117-162.

'236	Russ (EX1005)
48[pre]. A method to process media content provided by a primary security system, the method comprising:	See claim 140. The conditional access client (<i>e.g.</i> , client-receiver 122) processes media content from a primary security system (<i>e.g.</i> , service instances from headend 102). Wasilewski, ¶¶118-120.
48[a]. receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data	See claims 140[a.i]-140[a.ii].

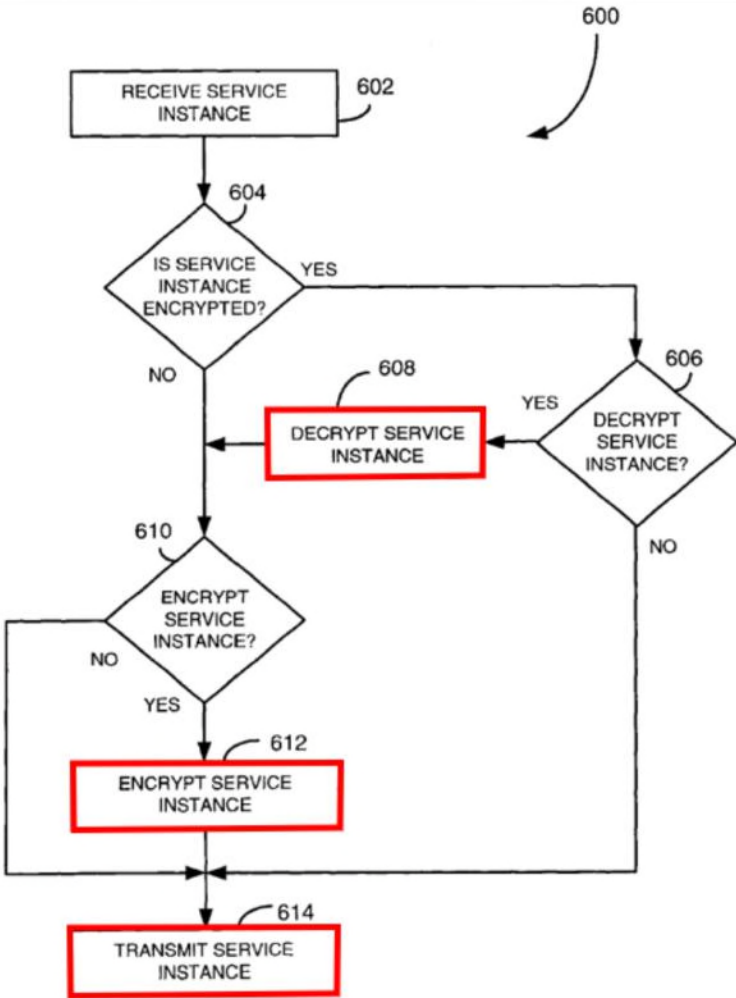
'236	Russ (EX1005)
<p>that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain,</p>	
<p>48[b.i]. wherein the primary security 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</p>	<p>See claim 140[c.i].</p>
<p>48[b.ii]. the conditional access server</p>	<p>See claim 140[c.ii].</p>

'236	Russ (EX1005)
<p>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</p>	
<p>48[b.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.</p>	<p>See claim 140[c.iii].</p>
<p>49[pre]. The method of</p>	<p>See claim 48.</p>

'236	Russ (EX1005)
claim 48,	
49[a]. wherein the security message is an entitlement message; and	See claim 141[a].
49[b]. wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.	See claim 141[b].
50. The method of claim 48, wherein the access controlled format protects access to data using a digital rights management system.	See claim 142.
57. The method of claim 50, wherein the access controlled data comprises a result of	<p>Russ discloses that the access controlled data comprises a result of descrambling media content (<i>e.g.</i>, DSCT 110 encrypts and transmits the decrypted service instance to client-receiver 122) scrambled by a conditional access system of the primary security system (<i>e.g.</i>, the service instance was scrambled by headend 102). Wasilewski, ¶¶129-132.</p> <p>DSCT 110 receives service instances from headend 102. Russ,</p>

'236	Russ (EX1005)
<p>descrambling media content scrambled by a conditional access system of the primary security system.</p>	<p>7:56-58. Prior to transmission to DSCT 110, service instances are encrypted with control words and/or with a Digital Video Broadcasting (DVB) Common Scrambling technique. Russ, 12:47-13:19. Wasilewski, ¶131.</p> <p>DSCT 110 descrambles received service instances, encrypts descrambled service instances according to the encryption scheme determined between DSCT 110 and client-receiver 122, and transmits the encrypted descrambled service instances to client-receiver 122. Russ, Fig. 6, 15:46-52, 16:64-17:14, 19:50-20:19. Wasilewski, ¶130.</p> <p><i>E.g.,</i></p> <p>Regarding data having been scrambled by headend 102:</p> <ul style="list-style-type: none"> • 7:56-58 (“Before the <u>DSCT 110</u> receives and accesses service instances from the headend 102, the DSCT 110 is registered with the headend 102 and entitled to the service instances.”) • 12:47-13:19 (“In the preferred embodiment, <u>the multi-transport stream receiver-transmitter 228 is adapted to encrypt content prior to modulating and transmitting the content. Typically, the content is encrypted using a cryptographic algorithm such as the Data Encryption Standard (DES) or triple DES (3DES), Digital Video Broadcasting (DVB) Common Scrambling or other cryptographic algorithms or techniques known to those skilled in the art...</u> It is to be understood that for the purposes of this disclosure a “program” extends beyond a conventional television program and that it includes video, audio, video-audio programming and other forms of services and digitized content. “Entitled” DSCTs 110 are allowed to use the decryption information to decrypt encrypted content, details of which are provided hereinbelow. <p><u>The multi-transport stream transmitter/receiver 228 uses the MSK from the control system 232 to encrypt service instances.</u> The multi-transport stream transmitter/receiver 228 includes a counter that produces a numerical value</p>

'236	Russ (EX1005)
	<p>every couple of seconds or so and an encryptor. <u>The encryptor uses the MSK to encrypt the counter value to produce a control word. The control word is used by the encryptor as a key for encrypting a portion of the service instance.</u>")</p> <p>Regarding descrambling the scrambled data and encrypting the result for client-receiver 122:</p> <ul style="list-style-type: none"> • 15:46-54 ("<u>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>") • 16:64-17:14 ("<u>The memory 310 includes logic for dynamic encryption scheme determination. Generally, the content transmitted from the DSCT 110 to the client-receiver 122 is transmitted so as to protect the privacy of the communication. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium. [...] Non-limiting examples of dynamic encryption scheme determination logic include [...] Digital Transmission Content Protection (DTCP) [...].</u>") • Fig. 6

'236	Russ (EX1005)
	 <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>FIG. 6</p> <ul style="list-style-type: none"> • 19:50-20:19 (see claim 140[c.iii]) <p>See also:</p> <ul style="list-style-type: none"> • 13:20-39, 23:25-46, 23:55-67, claim 19
<p>82[pre]. A non-transitory machine readable medium containing executable</p>	<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 (e.g., software stored in memory and executed by a processor, secure element, and cryptographic device to implement logic steps) to process media content provided by a primary security system (e.g., to process service instances from headend 102; see claims 48,</p>

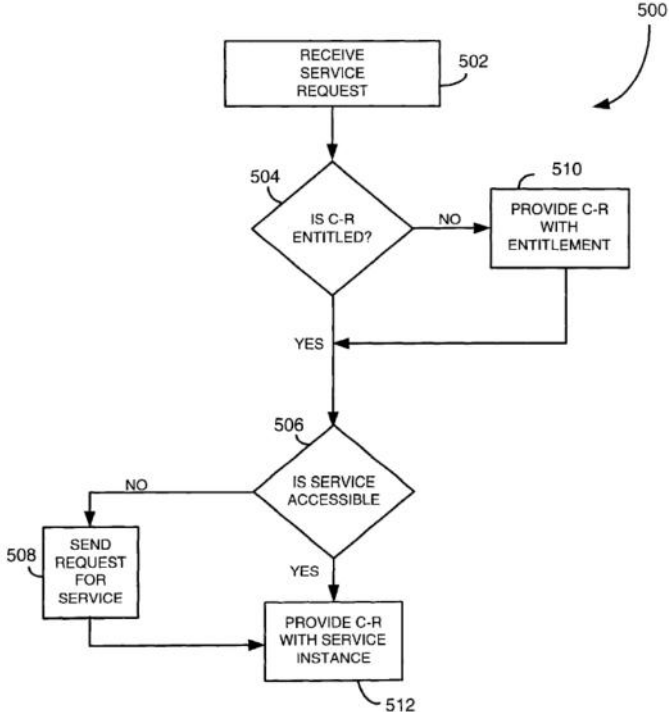
'236	Russ (EX1005)
<p>computer program instructions which when executed by a data processing system cause said system to perform a method to process media content provided by a primary security system, the method comprising:</p>	<p>140).</p> <p>Wasilewski, ¶¶134-137.</p> <p><i>E.g.</i>, Russ discloses:</p> <ul style="list-style-type: none"> • 3:23-40 (“The logic of the preferred embodiment(s) of the present invention can be implemented in hardware, software, firmware, or a combination thereof. In the preferred embodiment(s), the logic is implemented in software or firmware that is stored in a memory and that is executed by a suitable instruction execution system.”) • <i>See also</i> 16:13-26.
<p>82[a.i]. receiving, at a secondary conditional access client from a conditional access server through a network connection,</p>	<p><i>See</i> claim 140[a.i].</p>
<p>82[a.ii]. access controlled data that is in an access controlled format and that is at least partially derived from a</p>	<p><i>See</i> claim 140[a.ii].</p>

'236	Russ (EX1005)
security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain,	
82[b.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 140[c.i].</i>
82[b.ii]. the conditional access server authenticates clients of the conditional access server through a second authentication	<i>See claim 140[c.ii].</i>

'236	Russ (EX1005)
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	
82[b.iii]. wherein the conditional access server is configured substitute the first security domain with the second security domain for the clients under the second root of trust.	<i>See claim 140[c.iii].</i>
83[pre]. The medium of claim 82,	<i>See claim 82.</i>
83[a]. wherein the security message is an entitlement management	<i>See claim 141[a].</i>

'236	Russ (EX1005)
message; and	
83[b]. wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.	See claim 141[b].
84. The medium of claim 82, wherein the access controlled format protects access to data using a digital rights management system.	See claim 142.
84. The medium of claim 84, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary	See claim 57.

'236	Russ (EX1005)
security system.	
<p>116[pre]. A data processing system to process media content provided by a primary security system, the data processing system comprising:</p>	<p>Russ discloses a data processing system (e.g., digital broadband distribution system (DBDS) 100) to process media content provided by a primary security system (e.g., the DBDS 100 processes service instances, such as an audio/visual program provided by headend 102, e.g., by conditionally granting access to client-receiver 122).</p> <p>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. Service instances are, e.g., audiovisual programs provided by a primary security system including headend 102, with which DSCT 110 registers with and entitled to service instances by. Russ, 4:24-26, 7:56-58. Wasilewski, ¶¶149-151.</p> <p><i>E.g., Russ discloses:</i></p> <ul style="list-style-type: none"> Fig. 1: <p style="text-align: right;">FIG. 1</p>

'236	Russ (EX1005)
	<ul style="list-style-type: none"> • 4:24-26 (“<u>Service instances include ... an installment of an audio or visual or audio/visual program.</u>”) • 5:35-39 (see claim 140[pre]) • 7:56-58 (see claim 140[a.ii]) • 8:49-51 (see claim 140[pre]) • Fig. 5:  <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 style="text-align: center;">FIG. 5</p> <ul style="list-style-type: none"> • 17:61-18:66 (see claim 140[pre]) • See also 3:11-22, 4:21-39, 8:38-9:7, 19:7-42, 24:3-7, 24:37-38.
116[a]. means for receiving, at a secondary conditional	See claims 140[a.i]-[a.ii]. As explained for claims 140[a.i]-[a.ii], Russ discloses a secondary conditional access client comprising a communication interface (e.g., transceiver 902) to receive, from a conditional access server through a network connection,

'236	Russ (EX1005)
<p>access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain,</p>	<p>access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain.</p> <p>The transceiver 902 is therefore a “means for receiving, at a secondary conditional access client” such as a communication interface. <i>See</i> §VI.B.1 above.</p> <p>Wasilewski, ¶¶152-154.</p>
<p>116[b.i] wherein the primary security system authenticates the conditional access server clients of the primary security system</p>	<p><i>See</i> claim 140[c.i].</p>

'236	Russ (EX1005)
through a first authentication process using a first root of trust and	
116[b.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	See claim 140[c.ii].
116[b.iii]. wherein the conditional access server is configured to substitute the first security domain with	See claim 140[c.iii].

'236	Russ (EX1005)
the second security domain for the clients under the second root of trust.	
117[pre]. The data processing system of claim 116,	See claim 116.
117[a]. wherein the security message is an entitlement management message; and	See claim 141[a].
117[b]. wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.	See claim 141[b].
118. The data processing system of claim 116, wherein the access controlled format protects access to data	See claim 142.

'236	Russ (EX1005)
using a digital rights management system.	
125. The data processing system of claim 118, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.	See claim 57.

B. Ground 2: Claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 are Obvious Over Russ

Russ anticipates claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 as discussed in §VII.A above. Wasilewski, ¶¶164-165. To the extent PO argues that various features of Russ that are identified in the charts above are from distinct and unrelated embodiments—and would allegedly preclude a finding of anticipation—Russ further teaches that its disclosed features are combinable, and a POSA would have thus found the claims obvious as well.

As discussed in §VII.A.1 above, the various examples and embodiments disclosed in Russ are directly related to each other as non-limiting examples of implementations of the same system elements: **headend 102**, **DSCT 110**, **client-receiver 122**. As Russ explains, the “examples ... are merely examples among other possible examples,” described “embodiments ... are merely possible non-limiting examples of implementations, merely setting forth a clear understanding of the principles of the inventions,” and “changes, modifications, or 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, ¶166.

Accordingly, in light of the structures and functions identified in the claim charts in §VII.A.2-VII.A.3 above, which also apply here, claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 are obvious over Russ. Wasilewski, ¶167.

VIII. CONCLUSION

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

Dated: May 27, 2025

Respectfully submitted,

By: /Bas de Blank/

Bas de Blank, Reg. No. 74,930

ORRICK, HERRINGTON & SUTCLIFFE LLP

Counsel for Petitioner

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

I certify that on May 27, 2025, I will cause a copy of the foregoing document, including any exhibits or appendices filed therewith, to be served via Overnight FedEx at the following correspondence address of record for the patent:

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

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

M. Elizabeth Day	eday@bdiplaw.com
Marc Belloli	mbelloli@bdiplaw.com
Jerry D. Tice II	jtice@bdiplaw.com

Date: May 27, 2025

/Thomas A. James/
Thomas A. James Reg. No. 74,109
ORRICK, HERRINGTON & SUTCLIFFE
LLP

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing IPR petition contains 10,874 words excluding a table of contents, a table of authorities, Mandatory Notices under § 42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: May 27, 2025

/Thomas A. James/

Thomas A. James Reg. No. 74,109

ORRICK, HERRINGTON & SUTCLIFFE LLP