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. IPR2025-00882
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

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

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	*VideoLabs, Inc. et al. v. Hisense Co. Ltd. et al.*, 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	U.S. Patent No. 5,675,654
1015	RESERVED
1016	OMITTED
1017	*VideoLabs, Inc. v. ASUSTeK Computer, Inc.*, 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 100-109 and 111 ("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.*, IPR2024-01025, paper 12 (PTAB Dec. 9, 2024). However, that proceeding was terminated because of settlement by the parties there. *Id.*, paper 16

As to the '236, 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).

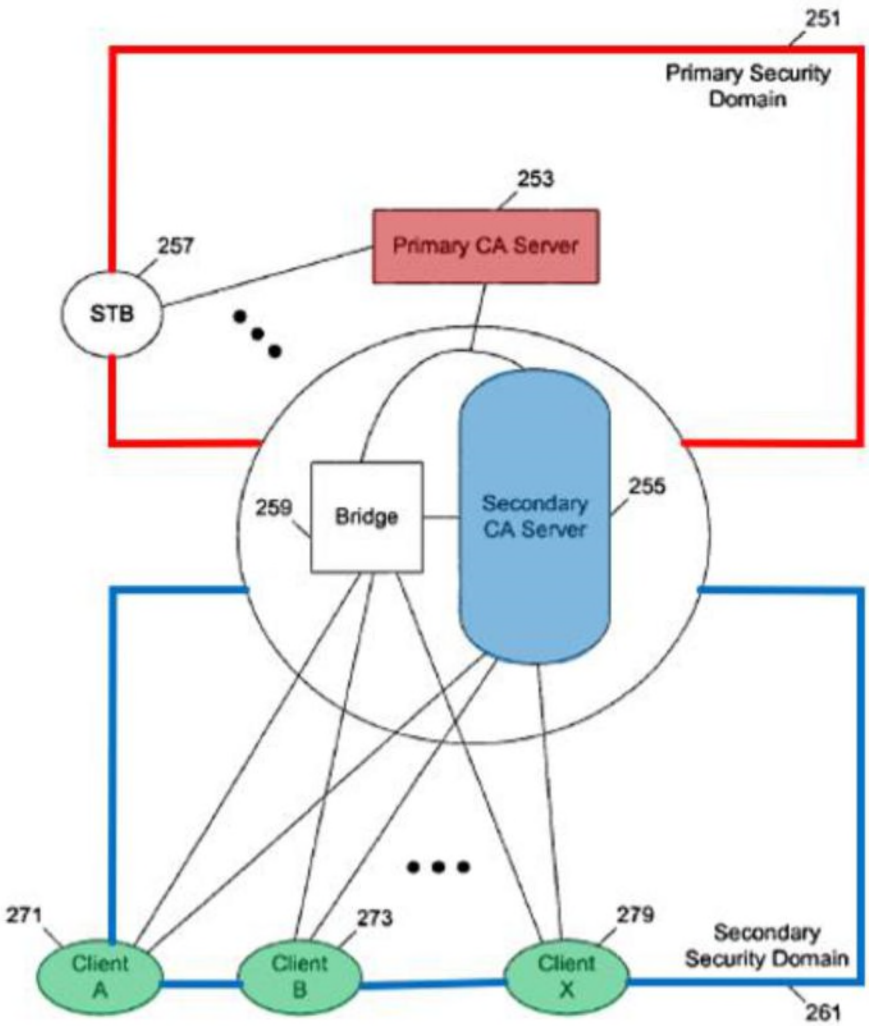


Fig. 2A

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**).

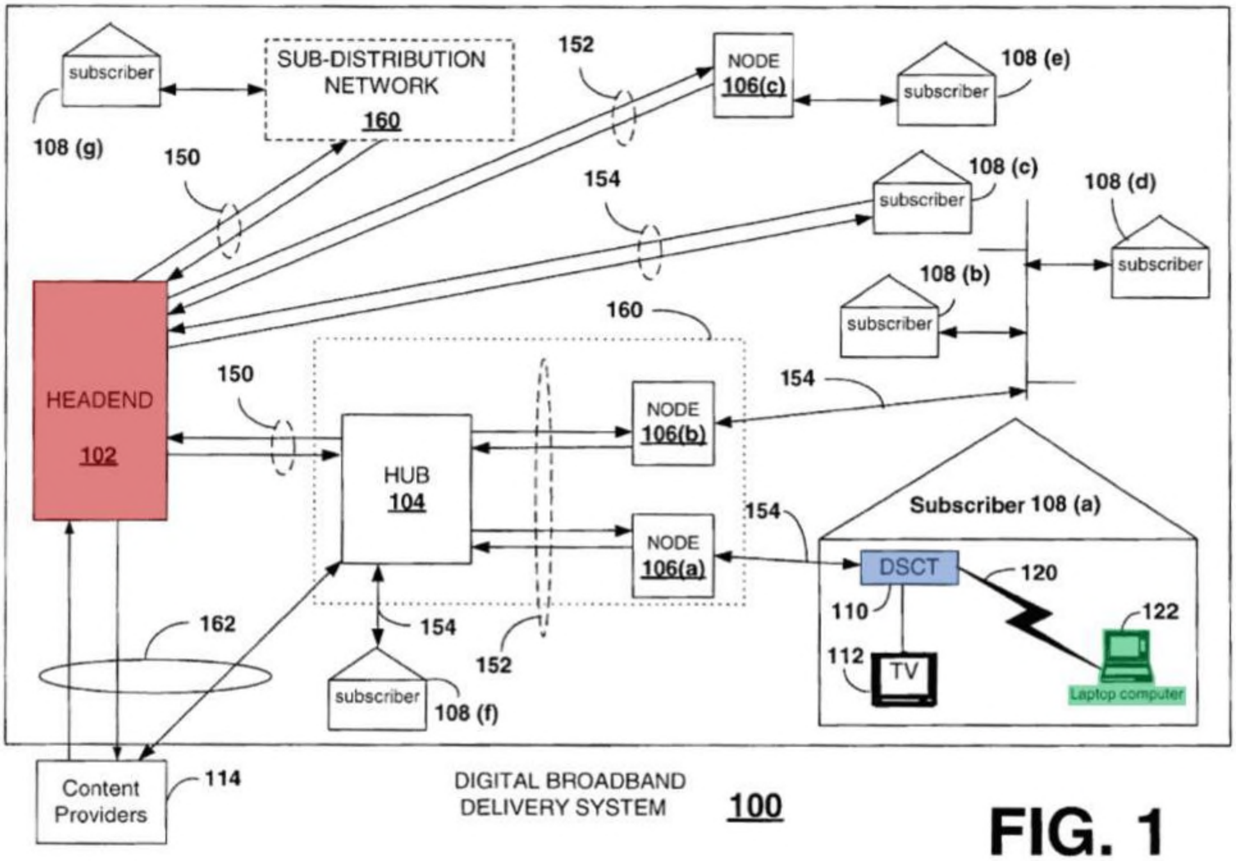


FIG. 1

Russ's system therefore bridges security systems, like the '236. Russ therefore anticipates 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. 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
VideoLabs, Inc. v. TCL Technology Corporation Group et al.	2:25-cv-00161	E.D. Tex.	2025-02-10
VideoLabs, Inc. v. Hisense et. al.	2:24-cv-00904	E.D. Tex.	2024-11-06
VideoLabs, Inc. v. HP Inc.	6:23-cv-00641	W.D. Tex.	2023-08-31
VideoLabs, Inc. v. ASUSTeK Computer Inc.	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.**
Hisense Co. Ltd. et al. v. VideoLabs, Inc.	8,291,236	IPR2025-00880
		IPR2025-00881
		IPR2025-00882
Hisense Co. Ltd. et al. v. VideoLabs, Inc.	8,667,304	IPR2025-00883

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

Lead Counsel	Bas de Blank, Reg. No. 74,930 Orrick, Herrington & Sutcliffe LLP 1000 Marsh Road Menlo Park, CA 94025 Email: M2BPTABDocket@orrick.com Phone: (650) 614-7400
Backup Counsel	Xiang Wang, Reg. No. 45,547 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 Richard Martinelli, Reg. No. 52,003 Orrick, Herrington & Sutcliffe LLP 51 West 52nd Street New York, NY 10019 Email: RFMPTABDocket@orrick.com Phone: (212) 506-5000 Thomas A. James, Reg. No. 74,109 Orrick, Herrington & Sutcliffe LLP 353 N Clark Street, Suite 3600 Chicago, IL 60654 Email: PTABDocketT6J1@orrick.com Phone: (312) 924-9800

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)
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	100-102, 106-107	Russ
3	§103	103-105	Russ in view of Robert
4	§103	108-109, 111	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.

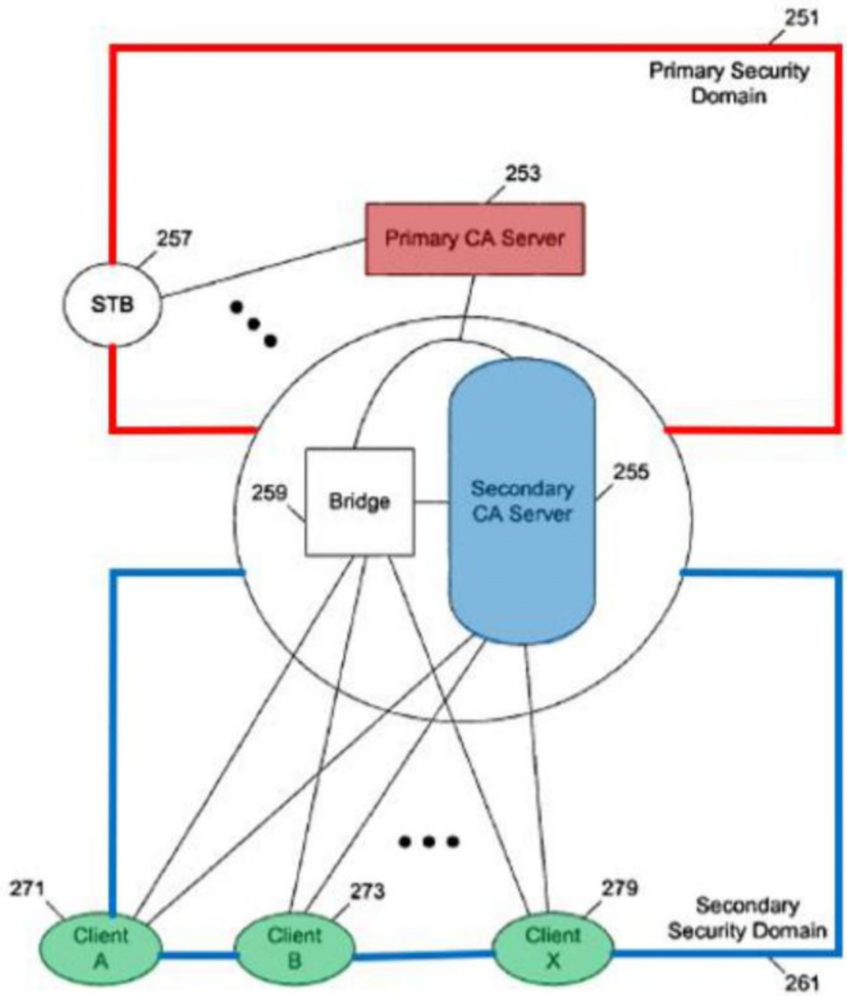


Fig. 2A

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.

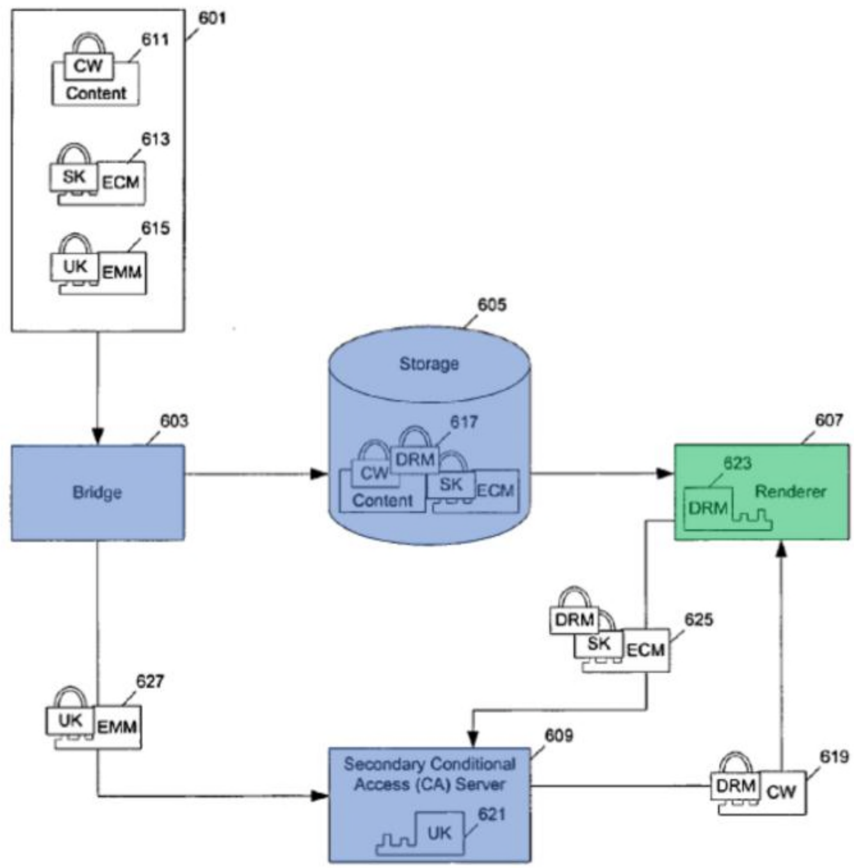


Fig. 11

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).[2] Only terms necessary

---

[2] The question of indefiniteness is not before the Board and is not a barrier to the Board's inquiry. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 813 (Fed. Cir. 2021);

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 the security messages"

Claim 100[c] recites "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 following figure:

Haas Automation, Inc. v. Olati LLC, IPR2021-00146, Paper 11 at 11-13 (PTAB May 18, 2021).

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, 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 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.

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.[3]

1. "means for receiving"

"Means for receiving, at a conditional access server" is recited at:

Claim	Text (functions of the means identified in bold)
100[a]	"means for **receiving, at a conditional access server, security messages of a primary security system in a first security domain**"

[3] Constructions of several *means* terms are disputed in related litigation not involving Petitioner. *See* EX1017, 23-37 (Please note that I'm changing to PDF page number not the brief page number.).

104[a]	"means for **receiving, at the conditional access server, an entitlement control message of the primary security system**"
106[a]	"means for **receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system**"
108[a]	"means for **receiving, at the conditional access server, an entitlement control message of the primary security system**"

The '236 describes "one or more communication interfaces" to receive the information such as security messages and ECMs. '236, claims 130[a], 133, 134, 136;'236FH, 99-101 (original claims).

Furthermore, the '236 describes that the secondary CA server receives EMMs, ECMs, and content directly from a primary security system or indirectly through a bridge and network connection, and also that the bridge may be combined "completely" with the secondary CA server. '236, 7:53-56, 17:26-27, 17:51-18:18, 21:21, 21:33-36, 21:50-52, 21:61-62, 22:33-37. Thus, with respect to combined bridges and secondary CA servers, bridges receive information from a primary security system via a "physical interface (285) [that] may be a tuner." '236, 8:41-44.

Accordingly, the structure in the specification linked to the claimed functions, "means for receiving, at a conditional access server…," includes one or more communication interfaces, a physical interface, a tuner, and statutory equivalents. Wasilewski, ¶¶53-56.

2. “means for processing”

“Means for receiving” is recited at:

Claim	Text (functions of the means identified in bold)	Algorithm
100[b]	“means for **processing the security messages on the conditional access server**”	Decrypting an EMM. ’236, 12:59-60, 13:44-45, 14:21-23, 17:44-46, 21:61-63.
104[b]	“means for **processing the entitlement control message on the conditional access server to obtain a control word of the primary security system**”	Decrypting an ECM to obtain a control word. ’236, 10:36-39, 12:59-61, 13:44-47, 13:60-62, 14:21-24, 17:44-47,18:48-50, 22:41-42.
108[b]	“means for **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**”	Decrypting an ECM and re-encrypting the ECM to generate a substitutive ECM. ’236, 13:30-34, 13:44-53, 20:42-51, 22:26-29.

The ’236 describes “a processor” to process security messages and to process ECMs to obtain a control word or to generate a substitutive ECM. ’236, claims 130[b], 133, 136; ’236FH, 99-101 (original claims). A microprocessor is an example of a processor. ’236, 24:9-27.

The identified functions are performed according to the algorithms identified in the table above.

Accordingly, the structure in the specification linked to the claimed functions, “means for processing…,” includes a processor, such as a microprocessor, programmed to perform the identified algorithms, and statutory equivalents. Wasilewski, ¶¶57-62.

3. **“means for transmitting”**

“Means for receiving” is recited at:

Claim	Text (functions of the means identified in bold)
100[c]	“means for **transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data**[4] **that is in an access controlled format and that is at least partially derived from the security messages**”

The ’236 describes “one or more communication interfaces” to transmit access controlled from the conditional access server to a secondary conditional access client through a network connection. ’236, claim 130[b.ii]. The one or more communication interfaces may also be the same interface as the “means for receiving” discussed in §VI.B.1. *See* claim 130[a] and 130[b.ii];’236FH, 99 (original claims, encompassing “one” communication interface embodiments).

Further, with respect to combined bridges and secondary CA servers (*see* §VI.B.1), bridges include a “physical interface (289) [that] may be a data network communication interface for transmitting the protected content to a client in the

[4] Every mapped structure in the grounds below transmits 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.

secondary security domain." '236, 8:46-49. Transmitted content includes, for example, content "convert[ed]… from one protected (e.g., encrypted) format to another protected (e.g., encrypted) format" by transcrambler 287. '236, 8:44-46.

Accordingly, the structure in the specification linked to the claimed function, "means for transmitting…," includes one or more communication interfaces, a physical interface, a data network communication interface, and statutory equivalents. Wasilewski, ¶¶63-66.

4. "means for decrypting"

"Means for decrypting" is recited at:

Claim	Text (functions of the means identified in bold)	Algorithm
101[d]	[said means for processing…comprises] means for **decrypting to obtain a service key of the primary security system**"	Decrypting an EMM to recover a service key. '236, 10:31-34, 13:44-45, 18:4-5, 18:39-40, 21:46-48.

The "means for decrypting" are included in the "means for processing," which includes a processor, such as a microprocessor, and equivalents thereof, as discussed in §VI.B.2 above. The '236 does not describe any other structure of the processor for decrypting to obtain a service key.

The identified function is performed according to the algorithm identified in the table above.

Accordingly, the structure in the specification linked to the claimed function, “means for decrypting…,” includes the processor, identified in §VI.B.2 above, programmed to decrypt an EMM to recover a service key, and statutory equivalents. Wasilewski, ¶¶67-70.

5. “means for descrambling”

“Means for descrambling” is recited at:

Claim	Text (functions of the means identified in bold)
106[b]	“means for **descrambling the scrambled content according to the entitlement control message**”

The ’236 describes a “descrambler (325) to descramble the content for secondary CA clients” using a control word recovered from an ECM. ’236, 10:36-46. Additionally, “a standard scrambler/descrambler can be … located on the conditional access” server for scrambling/descrambling based on a control word. ’236, 17:10-15.

The ’236 further describes a “transcrambler” to descramble and rescramble content. ’236, claim 138[d]; ’236FH, 101 (original claims); *see also* 8:39-46.

Accordingly, the structure in the specification linked to the claimed function, “means for descrambling…,” includes a descrambler, scrambler/descrambler, transcrambler, and statutory equivalents. Wasilewski, ¶¶71-74

6. “means for storing”

“Means for storing” is recited at:

Claim	Text (functions of the means identified in bold)
107[a]	"means for **storing, at the conditional access server, the content in an encrypted form**"

The '236 describes a "recorder" that records CA protected content at the secondary CA server. '236, 16:46-52. Additionally, a "storage" or "storage device" stores content in an encrypted form. '236, 13:4-12, 18:35-36, 18:53-54, 20:22-25, 22:62-64, 23:1-7, claim 135[a]; '236FH, 100 (original claim).

Accordingly, the structure in the specification linked to the claimed function, "means for storing…," includes a recorder, storage, storage device, and statutory equivalents. Wasilewski, ¶¶75-77.

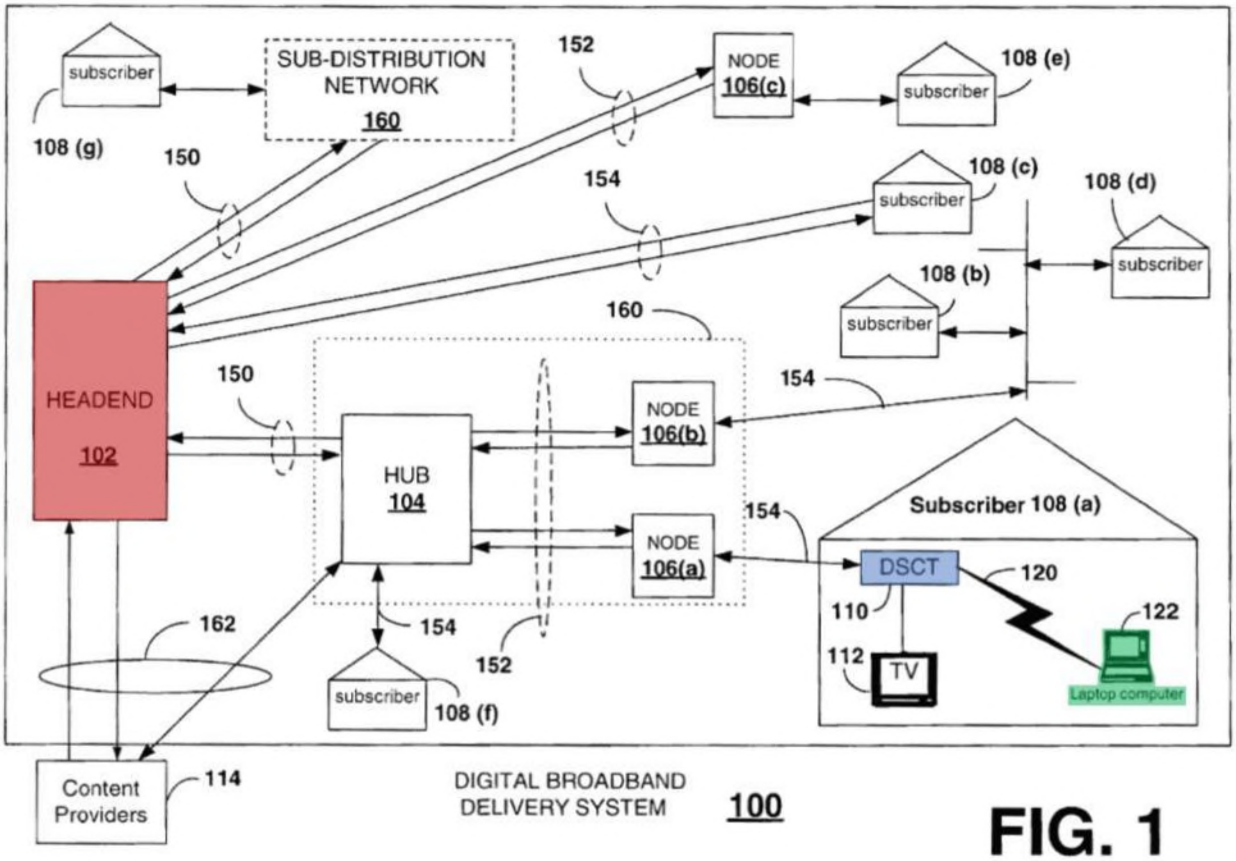
VII. GROUNDS OF UNPATENTABILITY

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, ¶¶1-224. The prior art renders the Claims unpatentable for reasons discussed below.

A. Ground 1: Claims 100-102 and 106-107 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:



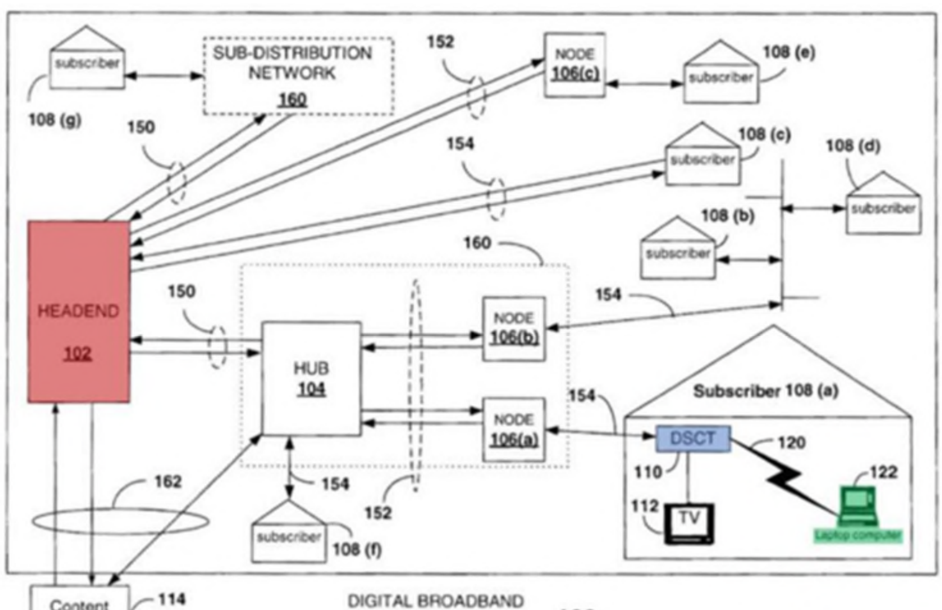
In digital broadband delivery system (DBDS) 100, **headend 102** communicates with content providers 114 to obtain services such as broadcasts or video-on-demand, and to subsequently serve them to subscribers. Russ, 5:35-51, 9:26-10:24, 13:5-9. For example, **headend 102** services subscriber location 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, ¶¶79-80.

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, ¶¶81-84.

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, ¶82.

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 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 100-102 and 106-107 of the ’236. Wasilewski, ¶¶94-176.

2. Claim Charts

’236	Russ (EX1005)
100[pre[5]]. A data processing system to process conditional access protection, the data processing system comprising:	**Russ discloses a data processing system** (*e.g.*, digital broadband distribution system (DBDS) 100) **to process conditional access protection** (*e.g.*, DSCT 100 of DBDS 100 grants conditional access entitlements to client-receiver 122). 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, ¶¶94-99. *E.g.*, Regarding a data processing system, including **DSCT 110** and **client-receiver 122**: • Fig. 1:  FIG. 1

[5] Regardless of whether the preamble (100[pre]) is limiting, the prior discloses it.

<table>
<tr><th>’236</th><th>Russ (EX1005)</th></tr>
<tr><td></td><td>

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

Regarding conditional access protection, *e.g.*, between **DSCT 110** and **client-receiver 122**:

- Fig. 5:

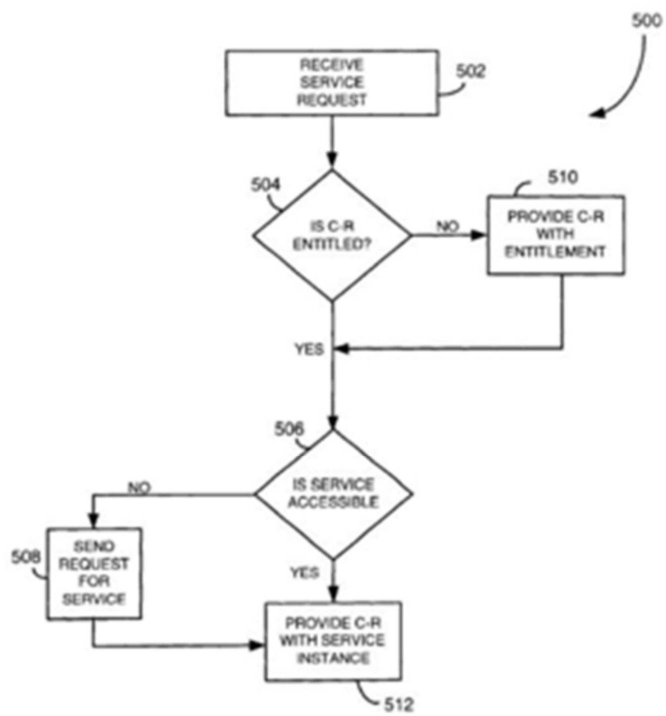


FIG. 5

- 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>….

</td></tr>
</table>

’236	Russ (EX1005)
	In step 504, the secure element 312… 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…. 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> <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>”) See also: • 3:11-22, 4:21-39, 8:38-9:7, 19:7-42, 24:3-7, 24:37-38
100[a]. means for receiving, at a conditional access server, security messages of a primary security system in a first security domain;	**Russ discloses means for receiving, at a conditional access server** (*e.g.*, input-port 302, tuner 304, transceiver 308 at DSCT 110, which is a conditional access server as discussed for claim 100[pre])**, security messages of a primary security system** (*e.g.*, to receive entitlement management messages (EMMs) of/from headend 102; EMMs include entitlement and key information) **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)**.** Wasilewski, ¶¶100-106. 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

<table>
<tr><th>’236</th><th>Russ (EX1005)</th></tr>
<tr><td></td><td>

security system in a first security domain in which **DSCT 110** is a member. Wasilewski, ¶¶104-105.

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; *see* ’236 claim 101 (security messages include EMMs). **DSCT 110** receives such communications on input-port 302 and transceiver 308. Russ, 13:53-56, 14:36-42. Wasilewski, ¶¶102-103.

Input-port 302 and transceiver 308 are therefore “means for receiving,” such as a communication interface or physical interface (*see* §VI.B.1) at a conditional access server (at DSCT 110, which is a conditional access server as discussed for claim 100[pre]).

E.g.,

Regarding a primary security system, including **headend 102**, in a first security domain with **DSCT 110**:

- Fig. 1

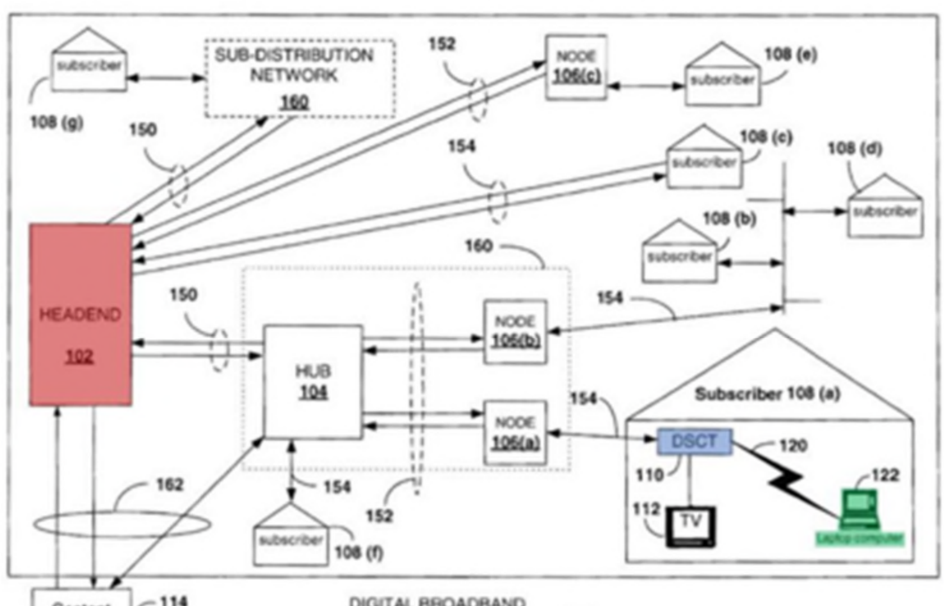


FIG. 1

- 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</u>

</td></tr>
</table>

’236	Russ (EX1005)
	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…. The content of a secure message may be encrypted…”) • 10:48-65 (“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 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.”) Regarding security messages, *e.g.*, EMMs of **headend 102**: • 8:25-34 (“DSCT 110… acts upon the EMM only if the EMM is authenticated as having come from the conditional access authority. 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.”)

’236	Russ (EX1005)
	Regarding **DSCT 110** receiving EMMs:

- Fig. 3

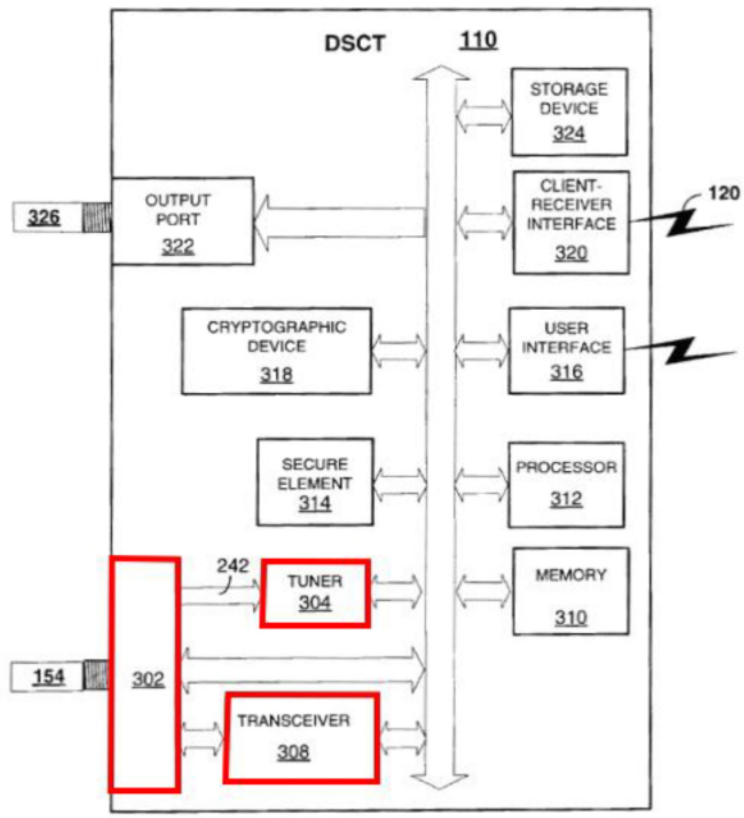
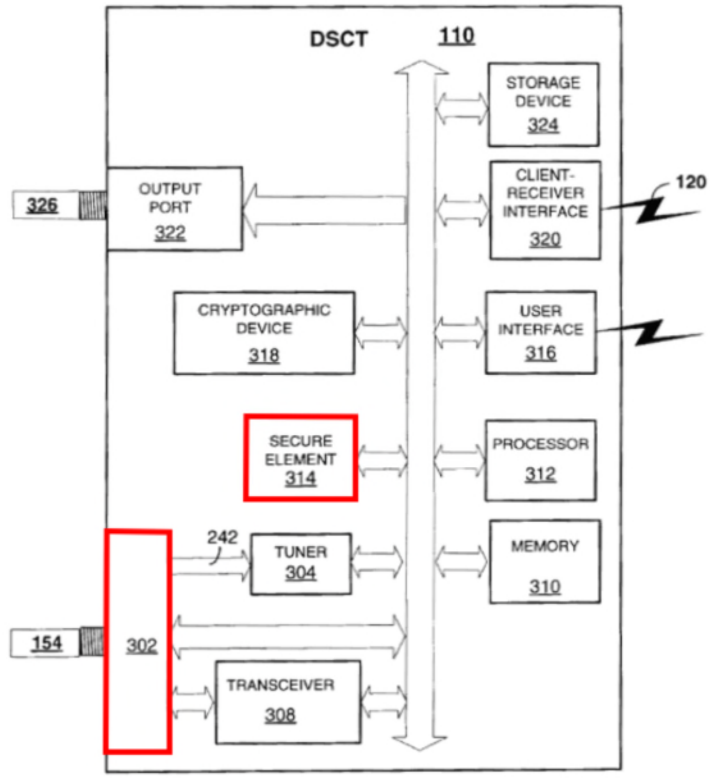
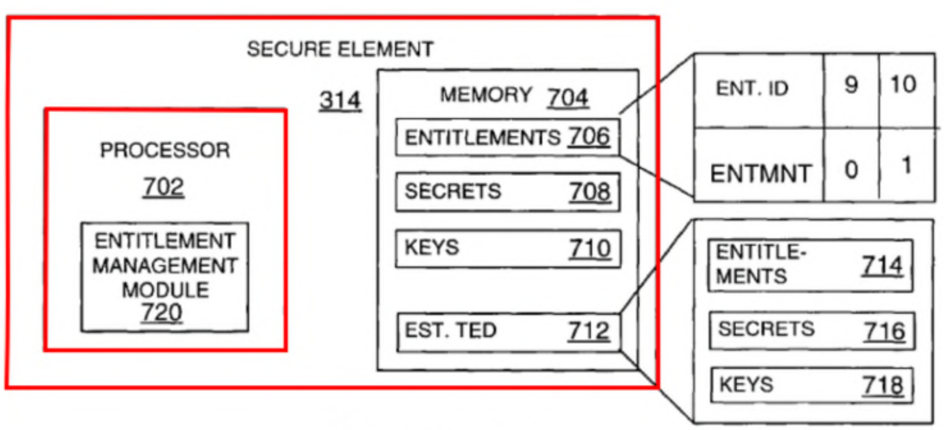


FIG. 3

- 13:53-56 (“<u>DSCT 110 is adapted to receive in-band and out-of-band communication at input-port 302</u> and output signals via output-port 322 and client-receiver interface 320.”)
- 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… secure messages such as EMMs. EMMs are sent to the secure element 314 for processing.…</u>”)

’236	Russ (EX1005)
	See also: • 7:7-20, 7:56-8:3, 10:39-56, 11:37-61
100[b]. means for processing the security messages on the conditional access server; and	**Russ discloses means for processing the security messages on the conditional access server** (*e.g.*, secure element 314 includes processor 702, is on DSCT 110, and is configured to decrypt EMMs)**.** 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 are sent to secure element 314 for processing by the AEMM, *e.g.*, for decrypting and authenticating EMMs. 14:36-42, 18:60-19:6, 21:11-21, 22:40-47. Wasilewski, ¶¶107-111. The secure element 314 is therefore a “means for processing” such as processor or microprocessor programmed to decrypt an EMM on the DSCT 110. *See* §VI.B.2 above. *E.g.* Regarding **DSCT 110** including means for processing: • Fig. 3

’236	Russ (EX1005)
	 FIG. 3 • Fig. 7:  FIG. 7

’236	Russ (EX1005)
	• 20:25-26 (“Referring to Fig. 7, the secure element 314 includes a processor 702 and a memory 704.”) Regarding processing EMMs: • 14:36-42 (*see* claim 100[a]) • 18:62-65 (“The secure element 314 of the DSCT 110 then processes the EMM….”) • 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… generates secure messages for the client-receiver 122. In the preferred embodiment, the 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.”) • 22:40-47 (“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, thereby converting the ciphertext content 804 to clear text content. The AEMM 720 uses the cleartext content and the authentication token 806 to authenticate the EMM.”) See also: • 18:60-19:6, 22:48-23:67, 24:25-36
100[c]. means for transmitting, from the conditional access server to a secondary conditional access client through a network	**Russ discloses means for transmitting, from the conditional access server to a secondary conditional access client** (*e.g.*, DSCT 110 further includes an output port 322 and client-receiver interface 320 to communicate with client-receiver 122) **through a network connection** (*e.g.*, client-receiver 122 joins DSCT 110’s network and communicates via communication link 120) **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

’236	Russ (EX1005)
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,	encrypt/decrypt the content and thus protect the content from unauthorized access)**, access controlled data that is in an access controlled format** (*e.g.*, 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** (*e.g.*, 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, ¶¶112-121. 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**. 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. The output port 322 is therefore a “means for transmitting” such as a communication interface, physical interface, or data network communication interface. *See* §VI.B.3. Wasilewski, ¶114. As discussed with respect to claim 100[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, 20:14-20. 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, ¶¶115-118. Examples of access controlled data transmitted between **DSCT**

’236	Russ (EX1005)
	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 client-receiver 122. Russ, 8:8-34, 15:46-52. Therefore, service instances are also partially derived from the security messages. Wasilewski, ¶117. *E.g.* Regarding means for transmitting information to **client-receiver 122** through a network connection: • •8:38-44 48 (“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… In alternative embodiments, the DSCT 110 is in communication… via… Ethernet….”) • 9:9-12 (“When… client-receiver 122 is brought into the local network, the client-receiver 122 discovers the network and communicates with the DSCT 110.”) • Fig. 3

<table>
<tr><th>’236</th><th>Russ (EX1005)</th></tr>
<tr><td></td><td>

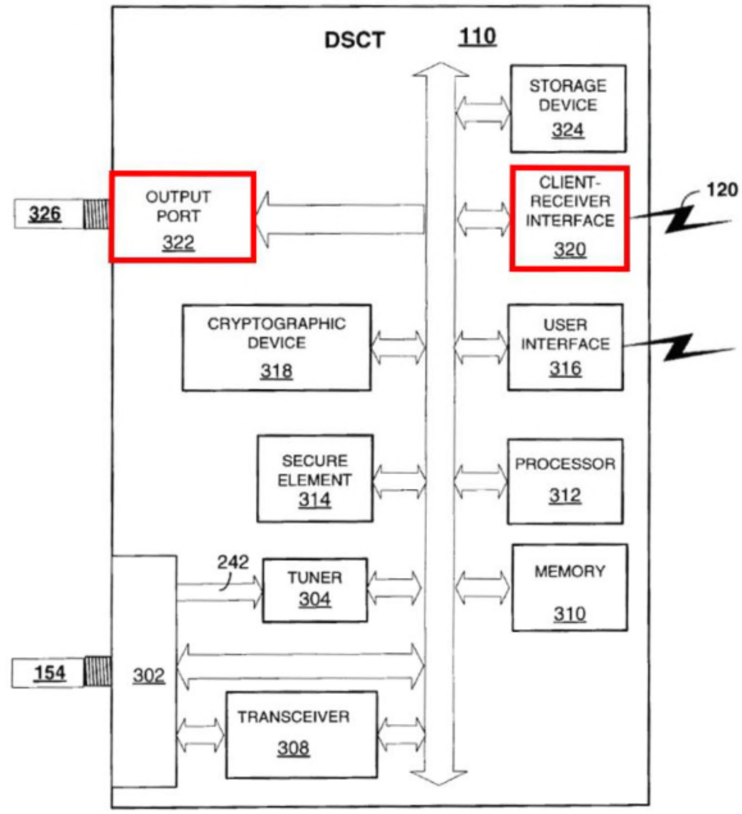


FIG. 3

- 13:53-65 (“<u>DSCT 110 is adapted to</u>… <u>output signals via output-port 322 and client-receiver interface 320</u>…. <u>[C]lient-receiver interface 320 includes a transceiver for a wireless communication link 120 between the DSCT 110 and a client-receiver 122.</u>

  In an alternative embodiment, <u>the client-receiver interface 320 includes a transceiver for a wired communication link….</u>”)

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

- Fig. 1:

</td></tr>
</table>

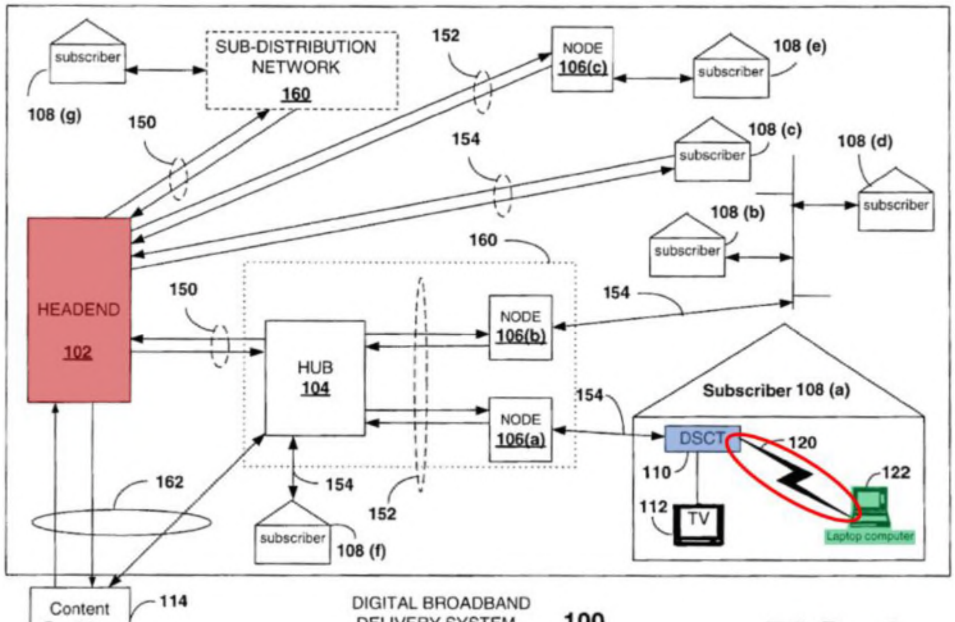
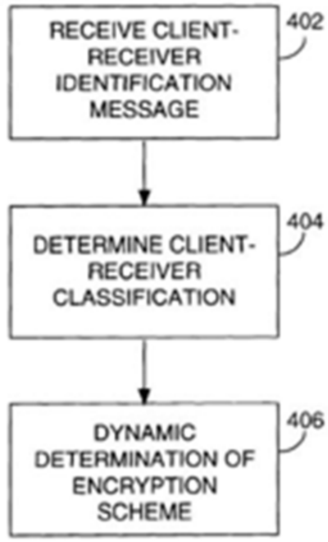
<table>
<tr><th>’236</th><th>Russ (EX1005)</th></tr>
<tr><td></td><td>


FIG. 1

16:64-17:14 (“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. The encryption scheme implemented by the DSCT 110 and the client-receiver 122 is determined by considering factors such as the device type of the client-receiver 122 and the communication medium….</u> Non-limiting examples… 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

</td></tr>
</table>

’236	Russ (EX1005)
	 **FIG. 4** ¶ • 17:15-34 (“[S]teps 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

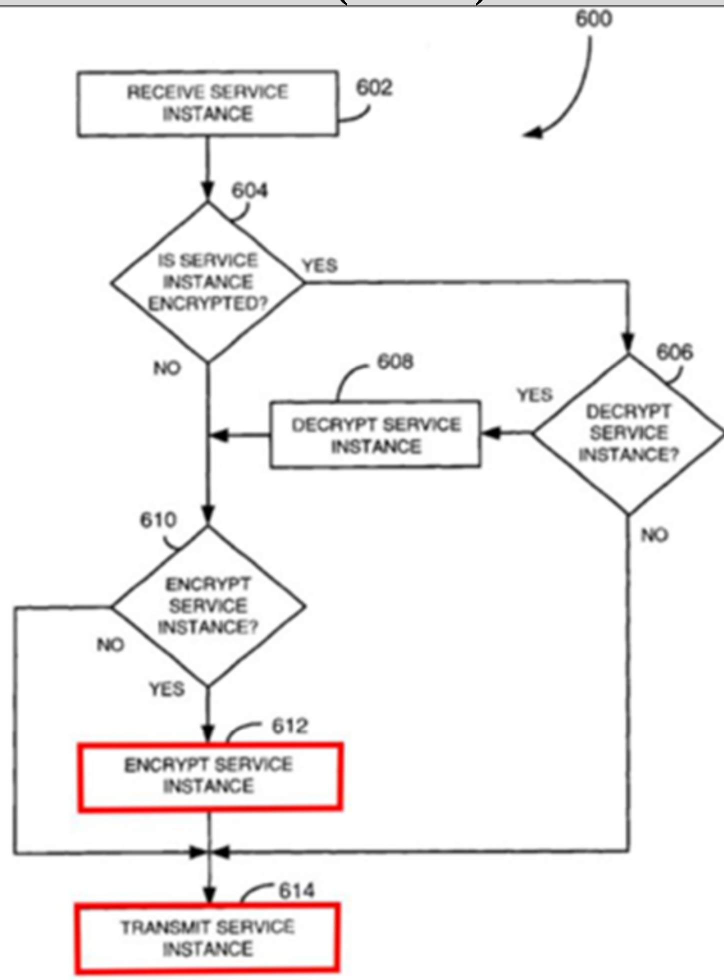
<table>
<tr><th>’236</th><th>Russ (EX1005)</th></tr>
<tr><td></td><td>


FIG. 6

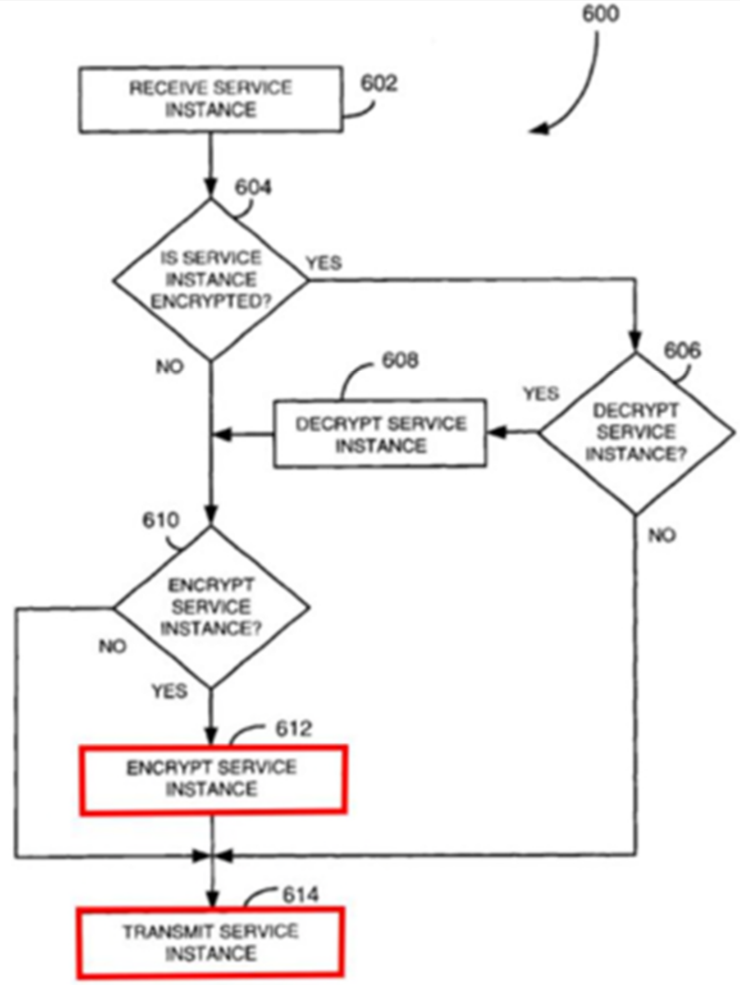
20:14-24 (“The cryptographic device 318 encrypts the service instance using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122….

[…] In step 614, the client-receiver interface 320 transmits the service instance to the client-receiver 122.”)
20:25-53 (“Referring to FIG. 7, the secure element 314 includes … a memory 704. The memory 704… includes entitlements 706, secrets 708, and keys 710. […]

The secrets 708 are secrets that are shared between the DSCT 110 and the client-receiver 122. In the preferred

</td></tr>
</table>

’236	Russ (EX1005)
	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.”) Regarding transmission of access controlled data to **client-receiver 122**: • 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…. 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.”) • Fig. 6

’236	Russ (EX1005)
	 **FIG. 6** • 20:14-24 (*see* above) • 21:11-21 (*see* claim 100[b]) • 21:22-65 (“<u>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.</u> The EMM 800 is an exemplary secure message. […]

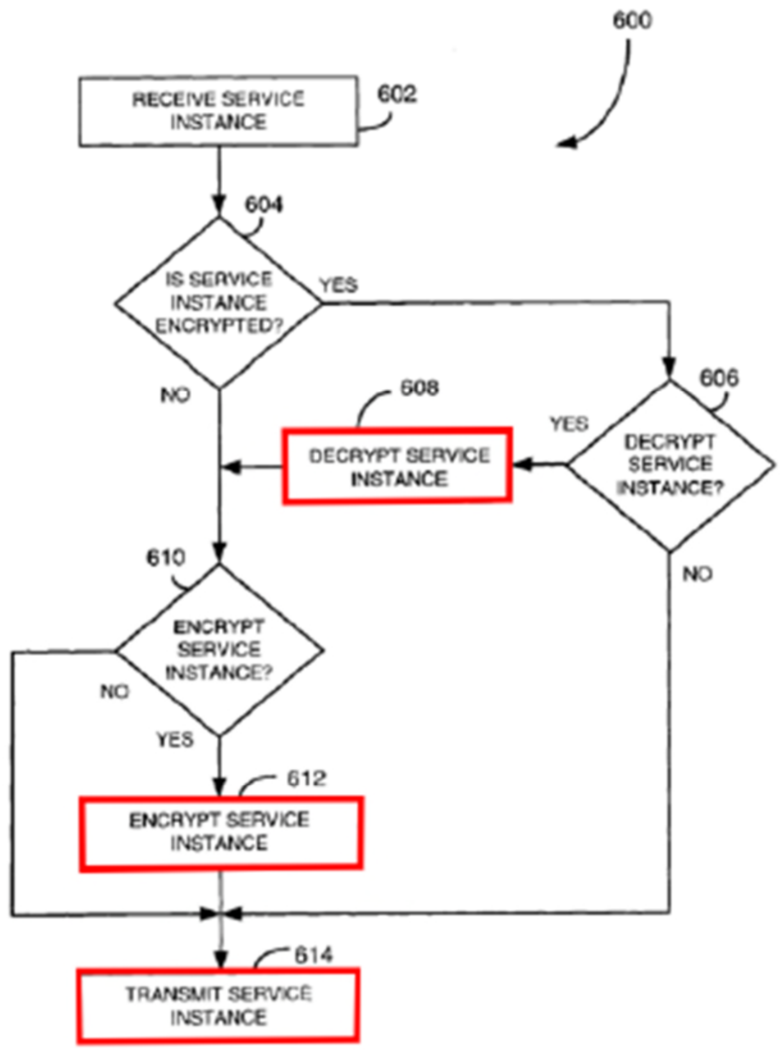
’236	Russ (EX1005)
	<u>Whether the message content 804 is encrypted depends upon whether or not privacy is desired.</u> … <u>Whereas, when the message content 804 is related to entitlements, or encryption, or decryption, then the message content 804 will probably be encrypted. Whether the message content 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>”) • 24:1-24 (“AEMM 720 includes logic for granting entitlements to the client-receiver 122 for service instances…. <u>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> The AEMM 720 can up date the client-receiver's entitlement map by <u>sending the client-receiver 122 an EMM with new entitlements</u> for the client-receiver 122.”) Regarding deriving access controlled data from security messages: • 8:8-22 (*see* claim 100[a]) • 8:25-34 (*see* claim 100[a]) • 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 (*see* above) See also: • 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 Additionally, to the extent PO argues that the access controlled format must be derived from the security messages (*see* §VI.A)—**Russ discloses the access controlled format partially derived from the security messages** (*e.g.*, headend 102 transmits an EMM to DSCT 110 dictating the encryption

’236	Russ (EX1005)
	scheme for communications with client-receiver 122). • 25:17-22 (“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.”) • *See also* 16:31-63, 19:7-27, 25:22-25.
100[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	**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.*, 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, ¶¶122-125. *E.g.*, “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 or entities. Wasilewski, ¶124. Regarding **headend 102** authenticating **DSCT 110** using a first root of trust: • 7:21-39 (“[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…. 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… is used for addressing messages to the DSCT 110. The

’236	Russ (EX1005)
	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.”) • 7:56-58 (*see* claim 100[a]) • 7:58-66 (“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.”) See also: • 7:40-55, 8:4-11, 10:39-47
100[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	**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 the second authentication process uses a second root of trust which is independent of and different than the first root of trust** (*e.g.*, 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 100[d.i])**.** Russ discloses that protocols for communication between

’236	Russ (EX1005)
authentication process uses a second root of trust which is independent of and different than the first root of trust, and	**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 100[c]. **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, ¶¶126-131. *E.g.*, Russ: • 16:64-17:14 (*see* claim 100[c])
100[d.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.	**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 100[d.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 service instance may be encrypted/decrypted by a multi-session key and CA control words (*see* Russ, 11:37-61, 13:14-34),

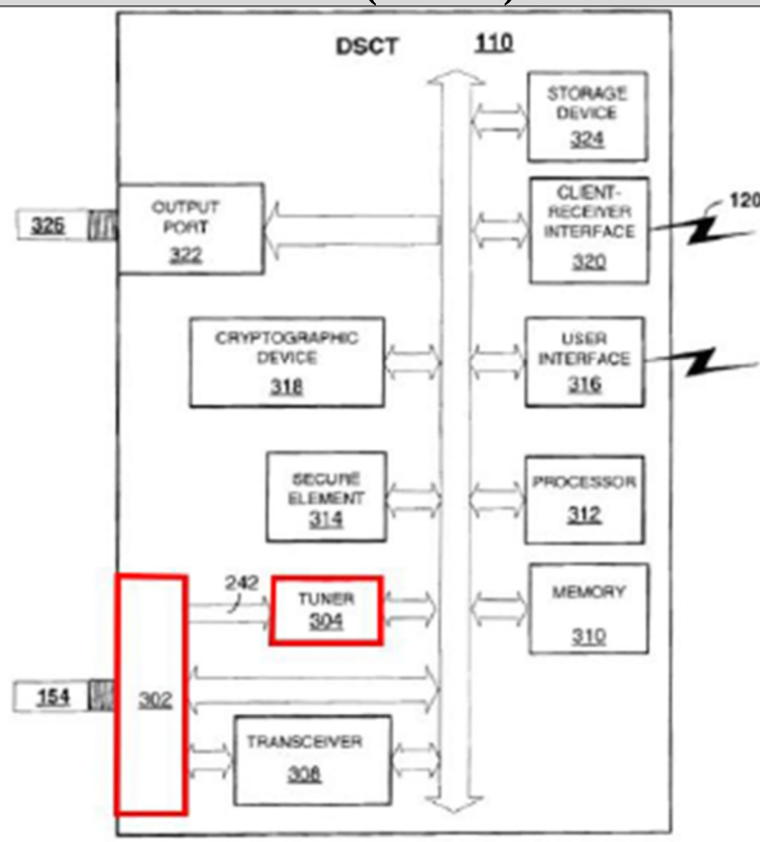
’236	Russ (EX1005)
	while the re-encrypted service instance is protected by DTCP encryption between **DSCT 110** and **client-receiver 122** (see discussion of claims 100[c, d.ii]). **DSCT 110** therefore substitutes the first security domain using CA with the second security domain using DTCP. Wasilewski, ¶¶132-137. *E.g.*, Regarding the first security domain including **headend 102** and **DSCT 110**: • 11:37-46 (multi-session key (MSK) used to generate control words, the MSK being transmitted to DSCT 110 in EMMs) • 13:14-34 (“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. 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.”) Regarding the second security domain including **DSCT 110** and **client-receiver 122**: • 16:64-17:14 (*see* claim 100[c]) • 17:15-34 (*see* claim 100[c]) Regarding **DSCT 110** substituting the first security domain for the second security domain: • 15:46-52 (*see* claim 100[c])

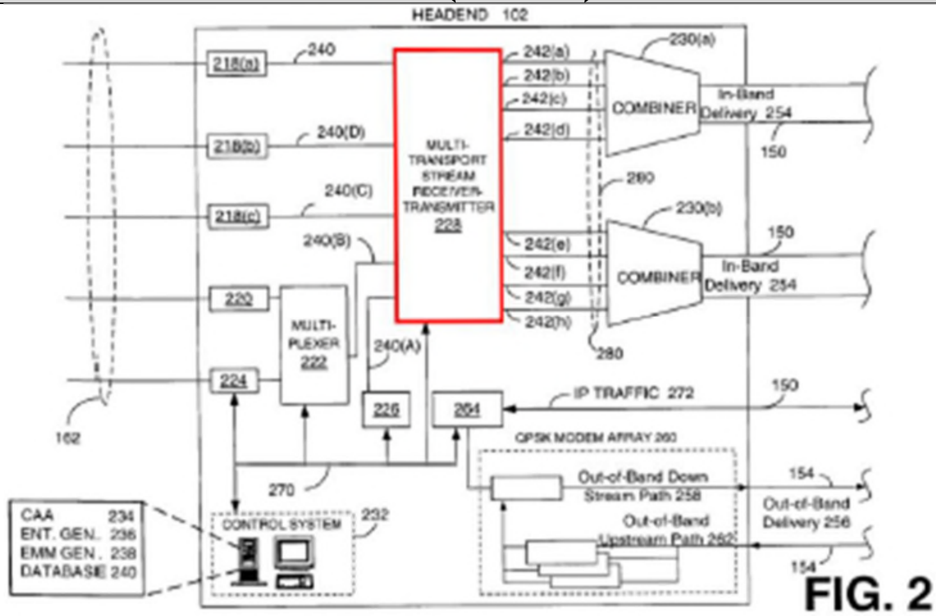
’236	Russ (EX1005)
	• Fig. 6  FIG. 6 • 19:52-20:16 (“[W]hen the processor 312 determines to decrypt the service instance…. <u>In step 608, the cryptographic device 318 decrypts to the service instance using the control word(s) provided by the secure element 314.</u> <u>In step 610, the processor 312 determines an encryption scheme for the selected service instance….</u> <u>The cryptographic device 318 encrypts the service instance using an encryption scheme that was dynamically</u>

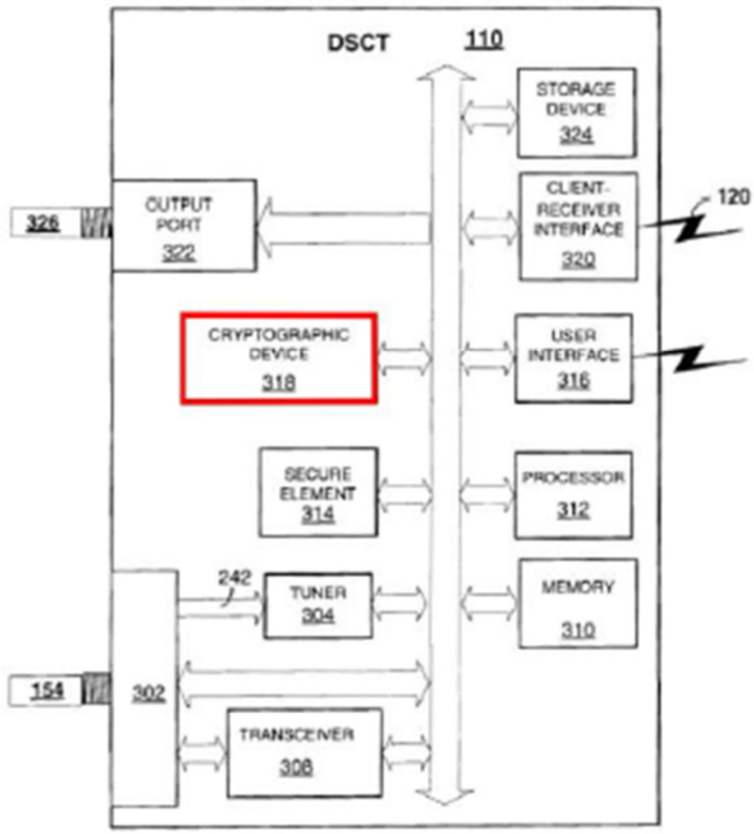
’236	Russ (EX1005)
	negotiated by the DSCT 110 and the client-receiver 122.”) See also: • 8:49-9:7, 23:47-67
101[pre.i]. The data processing system of claim 100,	*See* claim 100.
101[pre.ii]. wherein the security messages comprise entitlement management messages;	**Russ discloses that the security messages comprise entitlement management messages** (*e.g.*, DSCT 110 receives EMMs)**.** Russ discloses that **DSCT 110** receives security messages including EMMs from **headend 102**. Russ, 8:4-37, 10:48-65, 25:17-25; *see* discussions of claims 100[a] and 100[c]. Wasilewski, ¶¶139-141.
101[pre.iii]. the conditional access server has a user key representing a subscriber of the primary security system; and	**Russ discloses that the conditional access server has a user key representing a subscriber of the primary security system** (*e.g.*, 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, ¶¶142-144. *E.g.*, • 7:7-13 (“The headend 102 includes a database… that has the public key of each DSCT 110 in the DBDS 100. 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. ”) • 7:56-58 (*see* claim 100[a]) • 20:34-46 (“The keys 710 include a public key-private key pair for the DSCT 110…. The private key of the DSCT 110 is stored in the memory 704…. The holders of the DSCT's public key can use the public key… for encrypting

’236	Russ (EX1005)
	messages sent to the DSCT 110.”)
101[pre.iv]-101[a]. said means for processing the entitlement management messages comprises: means for decrypting to obtain a service key of the primary security system.	**Russ discloses that the means for processing the entitlement management messages comprises means for decrypting to obtain a service key of the primary security system** (*e.g.*, secure element 314 is configured to decrypt EMMs to obtain MSKs)**.** 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. The secure element 314 is therefore a “means for decrypting” such as a processor programmed to decrypt an EMM to recover a service key. *See* §VI.B.4 above. Wasilewski, ¶¶145-148. *E.g.*, • 10:48-65 (*see* claim 100[a]) • 11:37-46 (*see* claim 100[d.iii]) • 13:12-34 (*see* claim 100[d.iii]) • 22:40-45 (*see* claim 100[b])
102. The data processing system of claim 100, wherein the access controlled data is protected using a digital rights management system.	**Russ discloses that 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)**.** 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 100[d.ii]. A POSA would have recognized that DTCP is a form of digital rights management system. *See*, *e.g.*, 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, ¶¶149-151.

’236	Russ (EX1005)
106[pre]. The data processing system of claim 102, further comprising:	*See* claim 102.
106[a]. means for receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and	**Russ discloses means for receiving, at the conditional access server (***e.g.*, input-port 302, tuner 304 at DSCT 110**), 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)**.** Wasilewski, ¶¶153-158. Russ discloses that **DSCT 110** receives communications via input-port 302 and tuner 304. Russ, 13:53-56. Wasilewski, ¶155. **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, ¶¶156-157. **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, ¶157. The input-port 302 and tuner 304 are therefore “means for receiving,” such as a communication interface or physical interface (*see* §VI.B.1) at the conditional access server (at DSCT 110, which is a conditional access server as discussed for claim 100[pre]). *E.g.*, Regarding input-port 302 and tuner 304: • Fig. 3

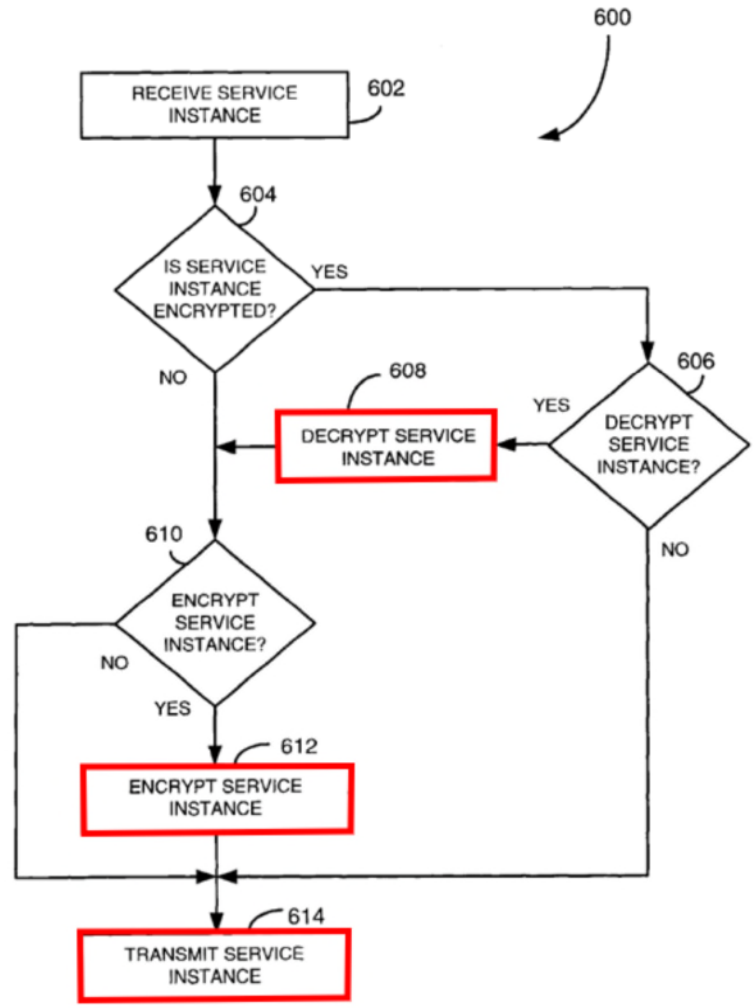
’236	Russ (EX1005)
	 FIG. 3 • 13:53-56 (*see* claim 100[a]) • 15:1-6 (“<u>tuner 304 receives in-band communication from input-port 302…. Typically, the tuner 304 also includes a demultiplexer for demultiplexing the received transport stream 242.</u>”) Regarding receiving ECMs and scrambled service instances of **headend 102**: • 7:56-58 (*see* claim 100[a]) • Fig. 2

’236	Russ (EX1005)
	 FIG. 2 • 12:47-13:11 (“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…”) • 13:14-34 (*see* claim 100[d.iii]) See also: • 5:52-6:7, 13:3-5
106[b]. means for descrambling the scrambled content according to the entitlement control message;	**Russ discloses means for descrambling the scrambled content according to the entitlement control message** (*e.g.*, cryptographic device 318 decrypts the service instance with control words generated from the ECM if DSCT 110 is entitled to the service instance according to the ECM)**.** Russ discloses that **DSCT 110** includes cryptographic device 318. Russ, Fig. 3. Cryptographic device 318 decrypts the service instance according to 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

’236	Russ (EX1005)
	control word to decrypt the service instance when **DSCT 110** is entitled to do so. Russ, 13:20-39, 15:46-52, 23:25-46, 23:55-67. Wasilewski, ¶¶159-164. Cryptographic device 318 is therefore a “means for descrambling,” such as descrambler or scrambler/descrambler. *See* §VI.B.5 above. *E.g.*, Regarding cryptographic device 318: • Fig. 3  FIG. 3 Regarding decrypting a service instance according to an ECM including a counter value and entitlement specifier:

’236	Russ (EX1005)
	• 13:12-34 (*see* claim 100[d.iii]) • 13:35-39 (“entitlement generator 236 associates each encrypted service instance, with 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.”) • 15:46-52 (*see* claim 100[c]) 23:25-46 (“Each encrypted service instant is associated with an element in the entitlement array. The entitlement specifier, which is included in the ECM for a given service instance, is used for determining an array element that has the entitlement of the DSCT 110 for the given service instance…. 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.”) • 23:60-67 (“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.”) See also: • 13:3-11, 15:27-32, 23:47-54
106[c]. wherein the access controlled data	**Russ discloses that the access controlled data comprises a result of descrambling the scrambled content** (*e.g.*, DSCT 110 encrypts and transmits the decrypted service instance to client-receiver 122)**.**

’236	Russ (EX1005)
comprises a result of descrambling the scrambled content.	Russ discloses descrambling or decrypting the service instance, as discussed for claim 106[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, ¶¶165-167. *E.g.*, Regarding descrambling the scrambled content and encrypting the result for **client-receiver 122**: • 15:46-52 (*see* claim 100[c]) • 16:64-17:14 (*see* claim 100[c]) • Fig. 6

’236	Russ (EX1005)
	 **FIG. 6** • 19:50-20:19 (*see* claim 100[d.iii]) See also: • claim 19
107[pre]. The data processing system of claim 106, further comprising:	*See* claim 106.
107[a].	**Russ discloses means for storing, at the conditional access**

’236	Russ (EX1005)
means for storing, at the conditional access server, the content in an encrypted form;	**server** (*e.g.*, DSCT 110 includes storage device 324 for storage)**, the content in an encrypted form** (*e.g.*, service instances are stored on storage device 324; service instances are encrypted)**.** 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. Stored service instances retrieved are encrypted. Russ, 15:16-26, 19:45-54. Storage 234 is therefore a “means for storing,” such as a storage, at the conditional access server. *See* §VI.B.6 above. Wasilewski, ¶¶169-173. *E.g.*, Regarding storage storing service instances: • Fig. 3

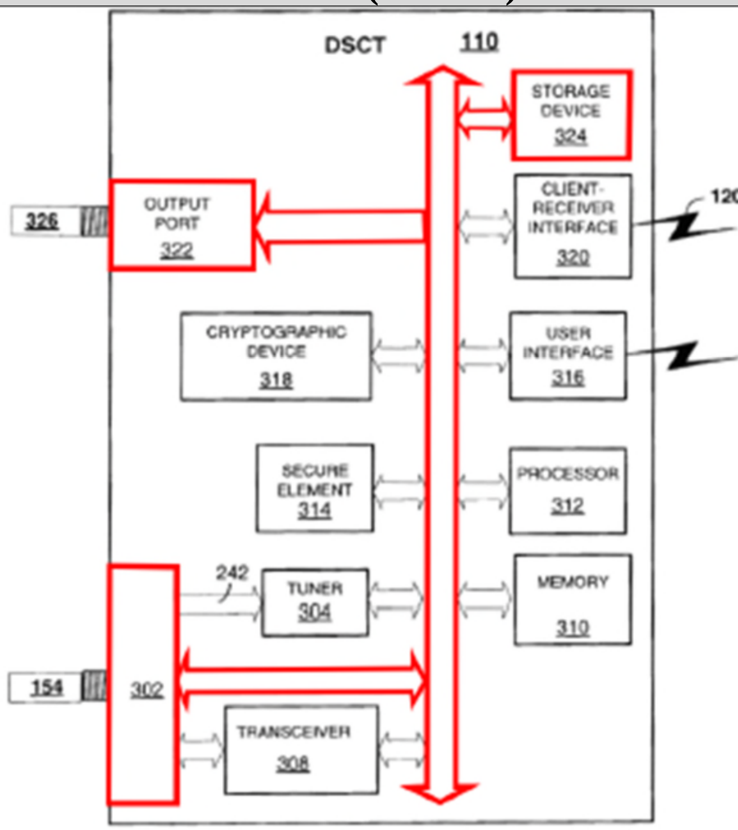
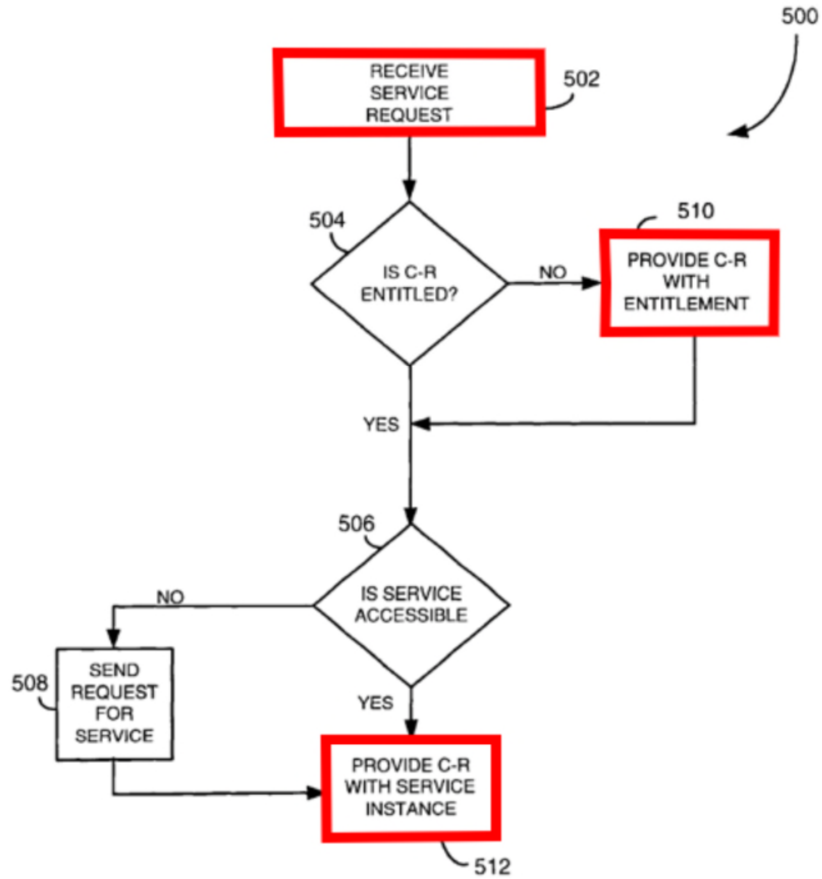
<table>
<tr><th>’236</th><th>Russ (EX1005)</th></tr>
<tr><td></td><td>


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 (“the selected service instance is stored on storage device 324 and is retrieved therefrom.

</td></tr>
</table>

’236	Russ (EX1005)
	In step 604, the processor 312… determine[s] whether or not the service instance is encrypted. If the selected service instance was encrypted at the headend, the processor 312 determines… whether the service instance should be decrypted.”) Regarding service instances being encrypted: • 15:16-26 (“[T]he transport stream 242 includes some service instances … that are encrypted…. [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 (*see* above) See also: • 13:12-14, 18:16-28, 19:47-65
107[b]. wherein the access controlled data is provided in response to a request from the secondary conditional access client.	**Russ discloses that the access controlled data is provided in response to a request from the secondary conditional access client** (*e.g.*, DSCT 110 transmits the EMM and service instance to client-receiver 122 in response to a request)**.** Wasilewski, ¶¶174-176. *E.g.*, • Fig. 5

’236	Russ (EX1005)
	 **FIG. 5** • 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…. [T]he secure element 314 generates an EMM, which includes the entitlement, 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 100[d.iii]), 20:22-24.

B. Ground 2: Claims 100-102 and 106-107 are Obvious Over Russ

Russ anticipates claims 110-102 and 106-107 as discussed in §VII.A. Wasilewski, ¶¶178-179. 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, ¶180.

Accordingly, in light of the structures and functions identified in the claim charts in §VII.A.2, which also apply here, claims 100-102 and 106-107 are obvious over Russ. Wasilewski, ¶181.

C. Ground 3: Claims 103-105 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, ¶¶85-87.

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.

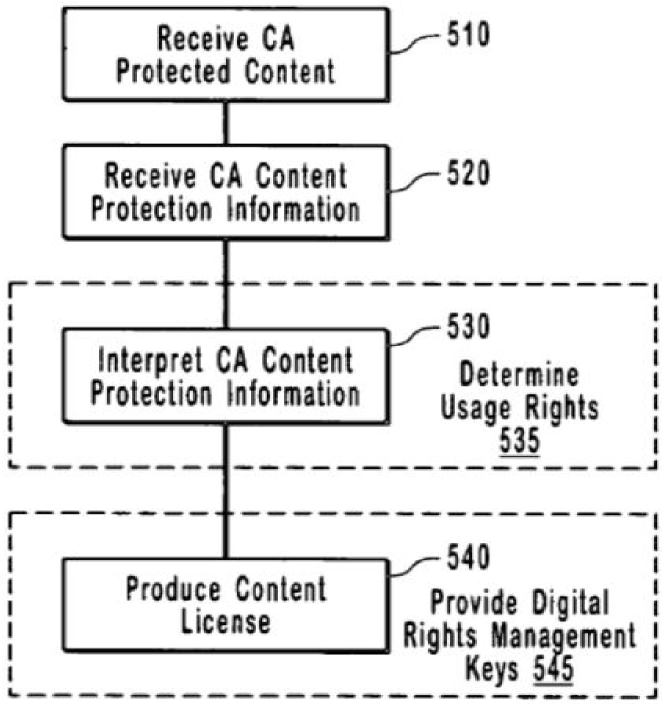


Fig. 5

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, ¶86.

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, ¶87.

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, ¶91.

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** 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 103) or for example what specific information or control words client-receiver 122 uses to decrypt service instances (*e.g.*, with respect to claims 104-105). 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, ¶182.

Regarding claim 103, 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, ¶183.

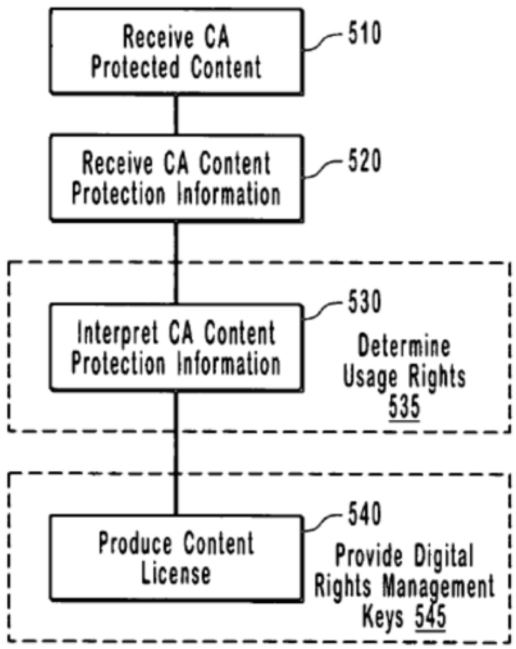
Regarding claims 104-105, Russ discloses that **client-receiver 122** decrypts service instances by generating control words. Russ, 26:16-28, 26:54-67. However, Russ leaves implementation details to the POSA regarding, for example, how **client-receiver 122** generates control words and/or whether **DSCT 110** transmits control words, control word indicators, counters, or ECMs to **client-receiver 122**—though Russ discloses that communications between **DSCT 110** and **client-receiver 122** are the negotiated protocols and encryption depending on **client-receiver 122's** hardware. Russ, 16:64-17:60, 20:12-17, 26:34-37, 26:54-64. As discussed above, Robert teaches that a variety of implementation options are available for accessing CA protected content on DRM devices. Robert, 8:56-11:59. For example, Robert teaches that access controlled data transmitted to a **destination device** includes the control words for decrypting content protected by DRM. Robert, 9:53-10:4. By providing the control words, which are obtained by decrypting received ECMs, the **destination device** can use a DRM license to decrypt CA-protected content. Robert, 4:27-33, 6:31-59, 9:66-10:4. A POSA would have therefore been motivated to implement Russ with implementation 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, ¶184.

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 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)).

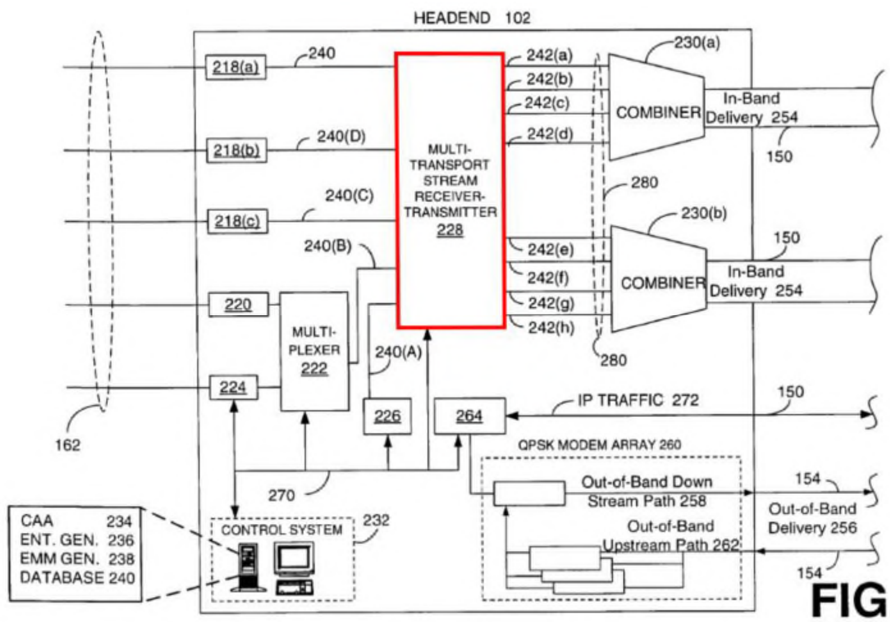
A POSA would have had a reasonable expectation of success implementing Russ's system by deriving rights from EMMs and including control words as access controlled data. Indeed, both Russ and Robert explain that content protection protocols and encryption schemes are well-known processes. Russ, 17:7-14; 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, ¶185.

3. Claim Charts

’236	Russ (EX1005) + Robert (EX1006)
103. The data processing system of claim 102, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.	**Russ discloses that rights to the access controlled data are at least partially derived from the entitlement management messages** (*e.g.*, DSCT 110 receives service instance entitlements in the EMM, then provides entitlements to client-receiver 122)**.** Wasilewski, ¶187. *E.g.*, • 17:61-18:66 (*see* claim 100[pre] in §VII.A.2; DSCT 110 grants entitlements to client-receiver 122) • 18:52-65 (*see* claim 100[c] in §VII.A.2) • *See also* 16:64-17:14, 21:11-21, 24:1-24, 21:22-65. **Robert discloses that rights to the access controlled data are at least partially derived from the entitlement management messages** (*e.g.*, 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). 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 100[d.ii]-[d.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 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, ¶¶188, 186-189.

’236	Russ (EX1005) + Robert (EX1006)
	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. 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

’236	Russ (EX1005) + Robert (EX1006)
	<u>upon the interpreted conditional access content protection information and in accordance with usage rights.</u>”) • *See also* 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)
104[pre]. The data processing system of claim 102, further comprising:	*See* claim 102 in §VII.A.2.
104[a]. means for receiving, at the conditional access server, an entitlement control message of the primary security system; and	*See* claim 106[a] in §VII.A.2.
104[b]. means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;	**Russ discloses means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system** (*e.g.*, secure element 314 of DSCT 110 is configured to encrypt a control word indicator of the ECM to obtain a control word generated by entitlement generator 236 of headend 102)**.** 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, 13:12-34. The control word 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

’236	Russ (EX1005) + Robert (EX1006)
	device 318. Russ, 23:55-67. Secure element 314 is therefore a “means for processing” such as processor or microprocessor programmed to decrypt an ECM to obtain a control word on the DSCT 110. *See* §VI.B.2 above. Wasilewski, ¶¶192-195. *E.g.*, • Fig. 2  FIG. 2 • 11:37-46 (*see* claim 100[d.iii] in §VII.A.2) • 13:12-34 (*see* claim 100[d.iii] in §VII.A.2) • 23:25-46 (*see* claim 106[b] in §VII.A.2) • 23:60-67 (*see* claim 106[b] in §VII.A.2)
104[c]. wherein the access controlled data comprises the control word.	**Robert discloses that the access controlled data comprises the control word** (*e.g.*, a receiver receiving a control word in a controlled access system transmits the control word to the destination device protected via DRM). In addition to Russ’s disclosure that **client-receiver 122** decrypts a service instance with a control word (*see* Russ, 26:16-28, 26:54-67), Robert teaches including CA control

<table>
<tr><th>’236</th><th>Russ (EX1005) + Robert (EX1006)</th></tr>
<tr><td></td><td>
words used by a client device to consume content (i.e., Russ’s 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 modify 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, ¶¶196-199.

E.g.,

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)

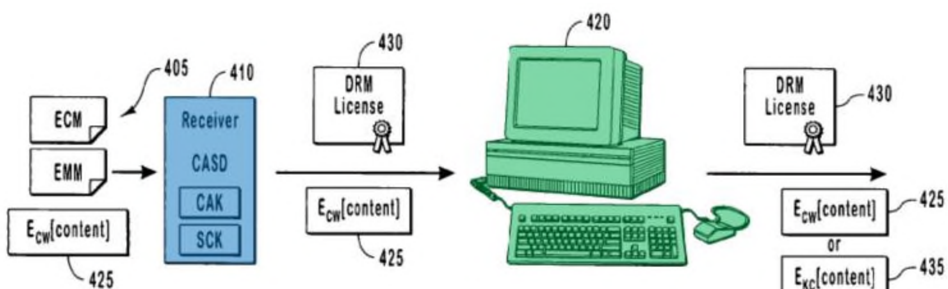


Fig. 4C

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…. [R]eceiver 410 is capable of producing or generating DRM license 430 and sending such license 430 to the destination DRM device 420…. <u>[R]eceiver 410 could have included the</u>

</td></tr>
</table>

’236	Russ (EX1005) + Robert (EX1006)
	appropriate keys (e.g., a list of CWs) in DRM license 430 when sent to destination device 420, such that destination device 420 can use the DRM license 430 to decrypt the CA-protected content 425 in it's original form.”) • *See also* 6:43-59.
105. The data processing system of claim 104, wherein the access controlled data comprises a decrypted version of the entitlement control message.	*See* claim 104, 104[c]. **Russ in view of Robert renders obvious that the access controlled data comprises a decrypted version of the entitlement control message** (*e.g.*, the ECM is decrypted, analyzed, and then its content protected under the DRM system transmitted to the destination device as access controlled data). Robert discloses that a **receiver 410** receiving an ECM with control words transcribes the control words into a DRM license such that the **destination device 420** can decrypt the CA-protected content with the control words. Robert, Fig. 4C, 6:31-69, 9:53-10:4; *see* claim 104, 104[c]. As Robert describes that this is alternative to providing the service keys used for encrypting the control words (*see* Robert, 6:31-59), a POSA would have recognized that the **receiver 410** decrypts the ECM to retrieve the control words—and not leave the control words in an encrypted version of the ECM—for transmission to the **destination device 420**. Wasilewski, ¶¶200-204.

D. Ground 4: Claims 108-109 and 111 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, ¶¶88-89.

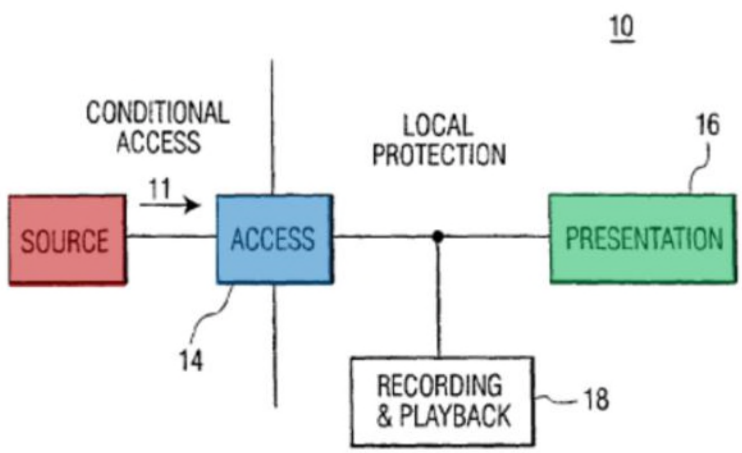


FIG. 1A

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.

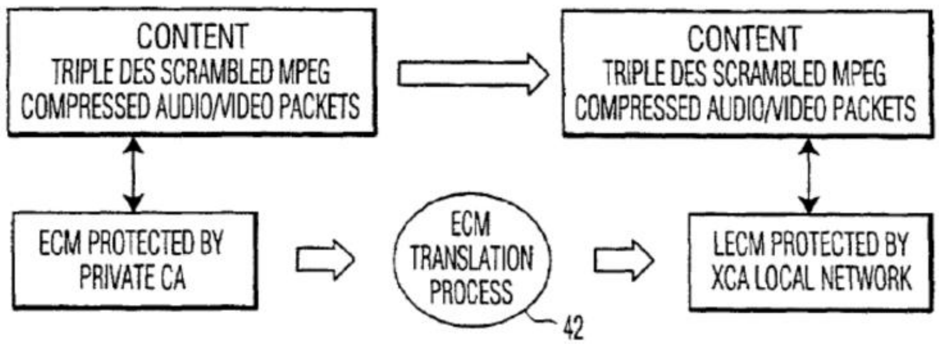


FIG. 4

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, ¶90.

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, ¶91.

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, ¶¶205-206.

As similarly 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 100[b] and 104[b] above) or by configuring an additional processor such as one taught by Eskicioglu, 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, ¶206.

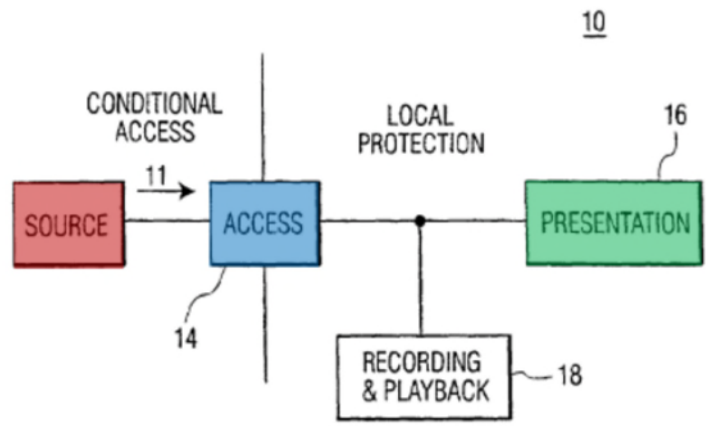
Furthermore, such implementation would have been, at least, the application of a known technique (*e.g.*, Eskicioglu's teachings of XCA protocols) to a known system ready for improvement (*e.g.*, Russ's disclosure of **DSCT 110** and **client-receiver 122** negotiating communications via any protocols 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)).

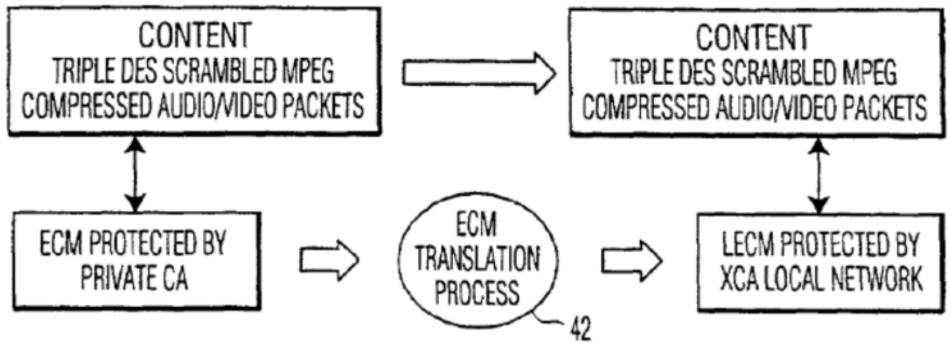
A POSA would have had a reasonable expectation of success implementing Russ's system with LECMs. Indeed, a POSA would have recognized that Eskicioglu's LECMs are structurally and functionally similar to well-known ECMs used in Russ. Additionally, the incorporation of ECM control words (*e.g.*, as taught 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, ¶207.

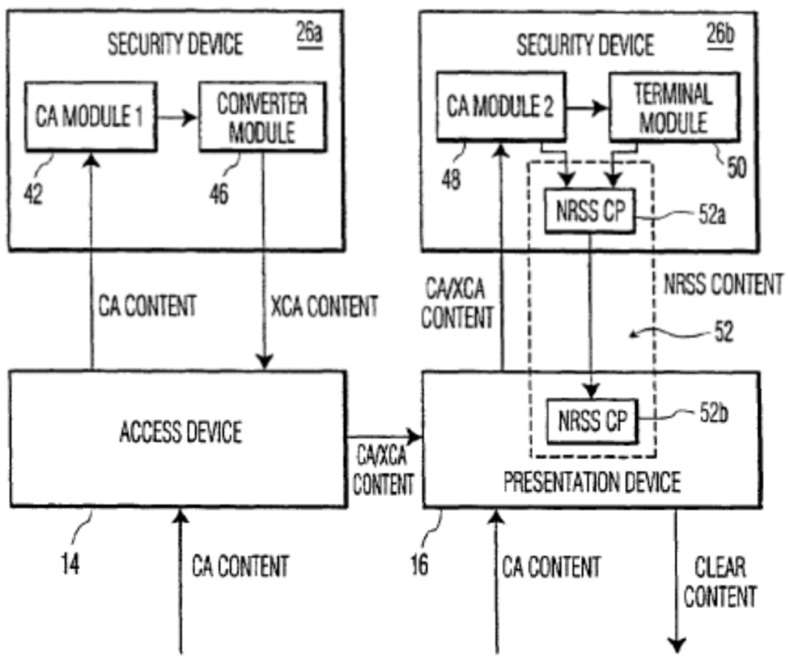
3. Claim Charts

'236	Russ (EX1005) + Eskicioglu (EX1007)
108[pre]. The data processing system of claim 100, further comprising:	*See* claim 100 in §VII.A.2.
108[a]. means for receiving, at the conditional access server, an entitlement control message of the	*See* claim 106[a] in §VII.A.2.

’236	Russ (EX1005) + Eskicioglu (EX1007)
primary security system; and	
108[b]. means for 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.	**Eskicioglu discloses means for processing the entitlement control message on the conditional access server** (*e.g.*, security device 26 is configured to decrypt and re-encrypt ECMs) **to generate a substitutive entitlement control message as a replacement of the entitlement control message** (*e.g.*, receiving an ECM, and processing the ECM to rebundle the ECM contents into a local ECM (“LECM”))**; wherein the access controlled data comprises the substitutive entitlement control message** (*e.g.*, the LECM is transmitted to the presentation device)**.** 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 (*see* 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, ¶¶210-214. Further, Eskicioglu's **access device**—analogous to Russ’s **DSCT 110** that includes means for processing including secure element 314 (*see* discussion of claims 100[b] and 104[b] above)—also operates with a smart card or converter card such as security device 26 for rebundling the ECM into the LECM. Eskicioglu, 4:46-50, 8:4-12. A POSA would have recognized that such cards include one or more processors used, *e.g.*, for cryptographic functions. *See* EX1014 (US 5,675,654), 1:61-2:3 (“an NRSS Smart Card includes a resident, programmable microprocessor and decryption engine”). Eskicioglu’s teaching of security device 26 and its functionality

’236	Russ (EX1005) + Eskicioglu (EX1007)
	is therefore a “means for processing” such as a processor programmed to decrypt and re-encrypt the ECM. See §VI.B.2 above. Wasilewski, ¶213. *E.g.*, • Fig. 1A (showing access device 14 receiving conditional access content that is to be presented locally on presentation device 16)  FIG. 1A • 4:46-50 (“Access devices typically operate… with an XCA/NRSS Converter Card…. The XCA/NRSS converter card creates XCA protected content from private [CA] protected content…”) • 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

’236	Russ (EX1005) + Eskicioglu (EX1007)
	 FIG. 4 • 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</u> a scrambled data component and <u>an encrypted descrambling key</u>; (b) <u>rebundling… said descrambling key</u> using a unique key associated with said first device, wherein said first device is an access device; (c) <u>receiving, in said second device</u>, said scrambled data component and <u>said rebundled descrambling key…</u>;”) • *See* also Fig. 5, 2:1-10, 4:25-27, 4:57-5:3, 8:19-47.
109. The data processing system of	*See* claim 108. **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**

’236	Russ (EX1005) + Eskicioglu (EX1007)
claim 108, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.	**conditional access server** (*e.g.*, the LECM is encrypted with the public key associated with the access device)**.** 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.e.*, 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, ¶¶215-217. *E.g.*, • 2:3-7 (“This method may comprise… <u>rebundling the descrambling key using a unique key associated with the first device</u>.”) • 7:41-46 (*see* claim 108) • Fig. 5  FIG. 5 • 8:19-30 (“The flow… 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</u>

’236	Russ (EX1005) + Eskicioglu (EX1007)
	<u>46 which generates the necessary LECM.</u>”) • See *also* Fig. 5, 4:57-5:3, 8:4-47, claim 1.
111. The data processing system of claim 109, wherein the entitlement control message and the substitutive entitlement control message have a same control word.	*See* claim 109. **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)**.** As discussed for claims 108[b] and 109, 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, ¶¶218-220.

VIII. CONCLUSION

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

Dated: May 27, 2025

Respectfully submitted,

By: <u>/*Bas de Blank*/</u>
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 13,799 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