

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU, INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner.

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

DECLARATION OF ANTHONY J. WASILEWSKI, PH.D.

Roku Exhibit 1003 Roku v. Videolabs
--

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
TABLE OF DOCUMENTS CONSIDERED	iii
I. INTRODUCTION	1
A. Background and Qualifications	1
1. Academic	2
2. Scientific-Atlanta & Cisco	2
3. Standards	3
4. Harmony	3
5. NGNA/DCAS/OpenCable	4
6. ATIS DRM	4
7. MPEG	5
8. CPTWG/DTLA/DTCP/HDCP	5
9. CableCARD™ (M-Card)	6
10. Patents	6
B. Documents and Information Considered	7
II. LEGAL STANDARDS	7
A. Anticipation	7
B. Obviousness	8
C. Claim Interpretation	9
III. BACKGROUND OF THE TECHNOLOGY	11
A. Content Protection	11
B. CAS	13
C. DRM	15
IV. THE '236 PATENT	16
A. Overview	16
B. Prosecution History of the '236 Patent	19
V. LEVEL OF ORDINARY SKILL IN THE ART	21
VI. CLAIM INTERPRETATION	22

A.	“access controlled data that is in an access controlled format and that is at least partially derived from the security messages”	22
VII.	OVERVIEW OF THE PRIOR ART	24
A.	Russ	24
B.	Robert	29
C.	Eskicioglu	31
D.	Analogous Art	33
VIII.	GROUND OF UNPATENTABILITY	33
A.	Ground 1: Russ anticipates claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135	34
1.	Invalidity of claims 130-131 and 134-135	34
2.	Invalidity of claims 32-34 and 38-39	67
3.	Invalidity of claims 66-68 and 72-73	72
B.	Ground 2: Russ renders obvious claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135	79
C.	Ground 3: Russ in view of Robert renders obvious claims 35- 36, 69-70, and 132-133	81
1.	Motivation to combine the teachings of Russ and Robert	81
2.	Invalidity of claims 132-133	85
3.	Invalidity of claims 35-36 and 69-70	88
D.	Ground 4: Russ in view of Eskicioglu renders obvious claims 40-41, 43, 74-75, 77, and 136-137	91
1.	Motivation to combine the teachings of Russ and Eskicioglu	91
2.	Invalidity of claims 136-137	94
3.	Invalidity of claims 40-41, 43, 74-75, and 77	96
IX.	CONCLUSION	101

TABLE OF DOCUMENTS CONSIDERED

Exhibit	Description
1001	U.S. Patent No. 8,291,236 (“’236 Patent”)
1002	File History of U.S. Patent Application No. 11/007,116 (“’236FH”)
1005	U.S. Patent No. 6,748,080 (“Russ”)
1006	U.S. Patent No. 7,546,641 (“Robert”)
1007	U.S. Patent No. 8,332,657 (“Eskicioglu”)
1008	<i>VideoLabs, Inc. v. Roku, Inc.</i> , Case No. 1:23-cv-01136 (D. Del.), Dkt. No. 1, Complaint Exhibit 11 – U.S. Patent No. 8,291,236 (“’236 Patent”) (Oct. 11, 2023)
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

I. INTRODUCTION

1. My name is Anthony J. Wasilewski. I have been retained on behalf of Roku, Inc. (“Roku”) to provide my opinions with respect to U.S. Patent No. 8,291,236 (EX1001; “the ’236 Patent”). In particular, I have been asked to provide my insights, analysis, and opinions regarding whether claims 32-36, 38-41, 43, 66-70, 72-75, 77, and 130-137 of the ’236 Patent (the “Challenged Claims”) are unpatentable over the prior art references identified below.

2. I submit this declaration in connection with Roku’s petition for *inter partes* review (“IPR”) of the ’236 Patent. I am being compensated for my time at my standard consulting rate. My compensation is not contingent upon the results of my analysis, the substance of my opinions, or the outcome of any proceeding involving the ’236 Patent. I have no financial interest in the outcome of this matter or any litigation between Roku and Patent Owner.

3. My analysis here is based on my years of education, research, and experience, as well as my investigation and study of relevant materials, including those cited herein.

A. Background and Qualifications

4. Based on my qualifications, education, knowledge, and experience, I believe I am qualified to offer opinions relating to the technology described in the ’236 Patent. A copy of my curriculum vitae, detailing my education and experience, is

submitted in this proceeding as EX1004. Additionally, the following overview of my background pertains to my qualifications for providing expert testimony in this matter.

1. Academic

5. My academic background includes a B.A. in Physics (Gettysburg College) and a Ph.D. in Astronomy (Case Western Reserve University). While this prepared me well for jobs that were not in the communications industry, I also acquired more general skills in software writing and knowledge of computing systems through my class and dissertation work. In my undergraduate classes, I wrote programs for calculus problems and other numerical analysis. I also wrote telescope control, data acquisition and data analysis software for work related to my Ph.D. dissertation. This latter work gave me a good understanding of device communications and elements of communications design.

2. Scientific-Atlanta & Cisco

6. The vast majority of my working career has been spent with Scientific-Atlanta (S-A) and later with Cisco Systems (Cisco acquired S-A in 2006). While some of my employment with S-A involved Radar Cross Section test gear development, the bulk of my time was spent in development of CATV, satellite and TelCo communications systems, in particular, audio-visual transmission networks and control systems.

7. At S-A, I wrote software for analog addressable control systems and led the development of the PowerKEY™ conditional access system – the first in the industry to use public/private key cryptography. I was the lead of the overall conditional access system design team and also directed a group of software developers in the creation of the S-A Digital Network Control System (DNCS) that functioned as the main digital subscriber communications terminal (DSCT) database, user interface, system configuration database and conditional access supervisor among other functions. I was also the PowerKEY™ Security Officer.

3. Standards

8. As early as the 1990s, the cable communications industry wanted greater interoperability in products from the various vendors they purchased from. I was a lead participant in many of the efforts to develop specifications to enable that interoperability.

4. Harmony

9. One of the earliest efforts to achieve this was the “Harmony” project to support interoperable conditional access between S-A and General Instrument (GI). GI included a conditional access system called DigiCipher™ in their products. Harmony was a jointly-defined architecture that involved secure control word sharing to achieve the desired interoperability between PowerKEY and DigiCipher. I was the S-A lead for the technical negotiations that produced the

Harmony specifications.

10. As Harmony was an agreement between just two DSCT/CAS vendors, the communications industry eventually desired a broader approach that would enable a multiplicity of vendors. Thus was born the Next Generation Network Architecture (NGNA) and Downloadable Conditional Access System (DCAS) efforts.

5. NGNA/DCAS/OpenCable

11. The development of NGNA/DCAS/OpenCable involved not only vendors but also CableLabs and two primary cable operators (Comcast and Time Warner Cable). NGNA specified the use of a flexible transport architecture, advanced video compression, Data Over Cable Service Interface Specification (DOCSIS) and the DOCSIS Set-top Gateway. DCAS, through a centralized Trusted Authority, enabled many DSCT providers, chip manufacturers and CAS vendors to interoperate in any DCAS-compliant system. The OpenCable Initiative produced the hardware and software specifications that allowed the CATV industry to deploy interactive services. I was the main S-A security contact for NGNA/DCAS and also participated in OpenCable including the OpenCable Application Platform (OCAP) effort.

6. ATIS DRM

12. The telephone industry, particularly AT&T and Verizon, also desiring

interoperable audio-visual networks, developed a set of specifications for an Interoperable IPTV System. This was done in a group called the IPTV Interoperability Forum (IIF), convened by the Alliance for Telecommunications Industry Solutions (ATIS). Part of that work focused on security functionality and digital rights management (DRM). I was the Co-chair of the IPTV Security Solutions (ISS) Task Force that produced documents that gave requirements for and standards for the deployment of interoperable IPTV systems and equipment. As a member of the ATIS IIF DRM Task Force, I made significant contributions to the end-to-end DRM Requirements specification.

7. MPEG

13. A critical enabling standard for commercial audio-visual services was developed by the Moving Picture Experts Group (MPEG-2) under the auspices of ISO/IEC. I participated in the MPEG-2 Systems Committee from Nov. 1992 to Nov. 1994 and authored many contributory papers and the Informative Annex C of ISO/IEC 13818-1. Several of my contributions to MPEG-2 were in the area of conditional access.

8. CPTWG/DTLA/DTCP/HDCP

14. The Copy Protection Technical Working Group (CPTWG) was convened by the motion picture and consumer electronics industries in anticipation of the digital coding and transmission of entertainment content. The work produced a DRM

specification for use in sending digital A/V content over local networks: Digital Transmission Content Protection (DTCP) and a licensing authority (DTLA) to administer and enforce use of the standard. Another standard was developed to similarly protect content as it is sent over device-to-device cables: High-bandwidth Digital Content Protection (HDCP). I was a representative from S-A and the CATV industry in these efforts and served as the S-A DTLA Security Officer.

9. CableCARD™ (M-Card)

15. A mechanism to enable retail availability of DSCTs, televisions and PCs that could run any CAS was mandated by the FCC and is known as the CableCARD or Multi-Stream M-Card. The CableCARD was a device that encapsulates the CAS functionality in a removable (PCMCIA) module. I was the lead S-A representative to the activity that defined the specifications for this module.

10. Patents

16. During my employment at S-A/Cisco I was an inventor on over 50 issued patents. These focused largely on telecommunications products and networks for transmission and reception of digital content. Three of these patents were deemed “essential” for MPEG-compliant implementations and were included in the license offered by the MPEG Licensing Authority (MPEG LA). Two of these MPEG patents deal with mapping of programs and CAS information within the Transport Stream.

17. I am also an inventor on patents dealing with Conditional Access Systems that offer protection for digital content both at rest (e.g. stored on Digital Video Recorders) and in motion (e.g. transmitted over CATV, TelCo and Satellite networks as well as in home networks).

18. Finally, I am an inventor on the Russ patent (US 6,748,080) which is cited as prior art in the present matter.

B. Documents and Information Considered

19. My opinions in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming these opinions, I have also reviewed the '236 Patent, its file history, and the documents listed in the Tables of Documents Considered above.

II. LEGAL STANDARDS

20. I am not an attorney, and I offer no opinions on the law itself. My understanding of the relevant principles this section is based on information provided to me by counsel.

A. Anticipation

21. I have been informed and understand that a patent claim is invalid as anticipated if each element of that claim is present either explicitly or inherently in a single prior art reference. I have also been informed that, to be an inherent disclosure, the prior art reference must necessarily disclose the limitation, and the fact that the reference might possibly practice or possibly contain a claimed

limitation is insufficient to establish that the reference inherently teaches the limitation.

B. Obviousness

22. I have been informed and understand that a patent claim can be considered to have been obvious to a person of ordinary skill in the art at the time of the alleged invention. This means that, even if all the requirements of a claim are not found in a single prior art reference, the claim is not patentable if the differences between the subject matter in the prior art and the subject matter in the claim would have been obvious to a person of ordinary skill in the art at the time of the alleged invention.

23. I have been informed and understand that a determination of whether a claim would have been obvious should be based upon several factors, including, among others:

- the level of ordinary skill in the art at the time the application was filed;
- the scope and content of the prior art; and
- what differences, if any, existed between the claimed invention and the prior art.

24. I have been informed and understand that the teachings of two or more references may be combined if such a combination would have been obvious to one having ordinary skill in the art. In determining whether a combination based on multiple references would have been obvious, it is appropriate to consider,

among other factors:

- whether the teachings of the prior art references disclose known concepts combined in familiar ways, and when combined, would yield predictable results;
- whether a person of ordinary skill in the art could implement a predictable variation, and would see the benefit of doing so;
- whether the claimed elements represent one of a limited number of known design choices, and would have a reasonable expectation of success by those skilled in the art;
- whether a person of ordinary skill would have recognized a reason to combine known elements in the manner described in the claim;
- whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; and
- whether the claimed invention applies a known technique that had been used to improve a similar device or method in a similar way.

25. I have been informed and understand that one of ordinary skill in the art has ordinary creativity and is not an automaton.

26. I have been informed and understand that in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the patent being considered.

C. Claim Interpretation

27. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill in the art of the patent at the time of the invention. I have been informed that patent claims generally should be interpreted consistent with

their plain and ordinary meaning as understood by a person of ordinary skill in the art in the relevant time period (*i.e.*, at the time of the purported invention, or the so called “effective filing date” of the patent application), after reviewing the patent claim language, the specification and the prosecution history (*i.e.*, the intrinsic record).

28. I have further been informed that a person of ordinary skill in the art must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history, the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office, and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner’s rejection, by clearly and unambiguously arguing to overcome or distinguish a prior art reference, or to clearly and unambiguously disavow claim coverage.

29. In interpreting the meaning of the claim language, I understand that a person of ordinary skill in the art may also consider “extrinsic” evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and

scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of those of skill in the art at the time of the claimed invention. This can be useful for technical terms whose meaning may differ from its ordinary English meaning. I understand that extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence, particularly if the applicant has explicitly defined a term in the intrinsic record.

30. I understand that certain claim terms may be interpreted to be “means-plus-function” terms. For these terms, I understand that there must be a corresponding structure disclosed in the specification in a way that a person of ordinary skill in the art would understand what structure would perform the claimed function. I understand the disclosure may be implicit in the specification if it would have been clear to a person of ordinary skill in the art what structure corresponds to the claimed function. With respect to a computer-implemented function, an algorithm must be disclosed in the specification. The means-plus-function claim terms would be interpreted as including disclosed structures and equivalents thereof.

III. BACKGROUND OF THE TECHNOLOGY

A. Content Protection

31. Community Antenna Television (CATV) systems began to be deployed in the late 1940s in the eastern United States as a way to get good TV pictures and

audio to areas that could not receive the existing over-the-air broadcasts. Typically, a receiving station (antenna) on a hilltop would be connected to homes in nearby valleys by two-conductor flat cables that transmitted the broadcast programming well enough for clear reception in the home of the few channels available at the time. At about the same time others in the western United States used coaxial cable to similarly re-distribute TV signals. By 1950, truly commercial CATV systems with regular monthly charges for connection were deployed. None of these systems used any security mechanisms and thus anyone who could connect to the network could get TV service without paying. This became an increasing problem.

32. To combat this signal-stealing issue, channel filters were used that would block any channel that was not being legitimately “subscribed” to. However, as the number of channels on the early CATV systems began to increase, the filter approach became unworkable. Also, the filters could be easily circumvented by determined “signal pirates”. The addition of interfering signals was then also tried and provided some security to the early systems. Over time, the growth of the number of systems and of subscribers lead the more advanced content protection technologies being utilized. Sync suppression of the analog video signal was used to cause television sets to not be able to display a clear picture without a special device being used to undo the suppression. These early devices (converters) were given to paying customers. Other analog video techniques such as line cut-and-

rotate, video inversion and sync inversion were eventually added. However, all of the analog protection techniques were relatively easy to reverse engineer and thus signal piracy still existed. With the advent of C-band satellite and terrestrial distribution of “premium” TV content (e.g. HBO and Showtime) in the 1970s and into the 1980s, the need for better signal security became paramount. Also, the need to be able to specifically authorize receiving devices, i.e. to address different authorization messages to different devices was crucial. These factors lead to the development of the early conditional access systems.

B. CAS

33. A conditional access system (CAS) is a collection of technologies and physical elements that are used to control access to audiovisual content (and possibly other data) in a networked environment. A CAS has a database of the devices that it can address individually to set authorization levels and other settings. Usually, the CAS is also connected to a billing system that associates the controlled devices with actual paying subscribers. Thus, the billing system directs the CAS to send the appropriate authorizations to the controlled devices. The controlled devices are known (for example) as Set-Top Terminals (STTs), Digital Subscriber Communications Terminals (DSCTs), Digital Terminal Adapters (DTAs), or CableCards. These devices are typically attached to TV displays and provide the means to transform audiovisual content that is protected and

inaccessible while moving across a network to clear content that can be displayed.

34. One of the earliest deployed CAS was VideoCipher I developed by Linkabit in 1983. It was used more in backhaul situations than in subscriber networks. For example, PBS and CBS used it to send content to affiliate stations. General Instrument acquired Linkabit in 1987.

35. VideoCipher I was followed by VideoCipher II and in the early 1990s by VideoCipher II Plus. These were used widely in terrestrial CATV systems and in satellite TV transmission. The video was still in analog format and thus was “scrambled” using some of the aforementioned methods but the indicator of which scrambling mode was in effect was sent in a digitally encrypted system message. During these years analog CAS were also developed by companies such as Scientific-Atlanta and were widely deployed in both terrestrial and satellite networks in the United States,

36. By 1994, the MPEG-2 specification for the coding and transmission of digital video and audio was approved as an international standard (ISO/IEC 13818).

37. In the mid to late 1990s, both General Instrument and Scientific-Atlanta developed and deployed fully digital CAS. The General Instrument (later Motorola) system was known as Digicipher™ and Scientific-Atlanta’s were PowerVu™ (satellite) and PowerKEY™ (CATV). In these systems, the now

digital video and audio could be encrypted (rather than scrambled) and this increased the security of the systems significantly. Also, authorization messages to controlled devices could be encrypted and, in the case of PowerKEY, digitally signed by the headend server. All of these systems depend on secure elements (chips) that are embedded in the controlled devices to ensure that secure messages, decryption keys and other system information would be processed and stored appropriately. Other satellite networks (DirecTV, Dish) were deployed with smaller ground antennas using Ku Band transmission and used other CAS (Dish uses Nagravision™ and DirecTV uses NDS VideoGuard™). All these systems protect access to content that is flowing over networks.

C. DRM

38. Digital Rights Management (DRM) systems evolved as the Internet was making transmission of perfect digital copies of artistic works very easy and widespread. This lead quite infamously to the open distribution of digital music without any payment or regard to the rights of the copyright holders. DRMs manage the access to digital works based on copyright or other legal grounds. They use some of the same techniques as CAS such as digital encryption and key management. But rather than encrypting the content as it flows into a network, a DRM encrypts the content while it is “at rest” (for example, on a DVD) and applies licensing rules to control access to the unencrypted version. An example is

the Content Scramble system (CSS) which used a relatively weak 40-bit key to encrypt the DVD content and was compromised just a few years after being released. Later DRMs, such Content Protection for Recordable Media (CPRM) and the Advanced Access Content System (AACS) used longer keys and better algorithms providing better protection for HD-DVD and Blu-ray content. However, it was still possible to discover (without license) some of the keys used in the encryption of the content due to the fact that software-based players (especially on PCs) are used to play the content and debuggers could be used to look for the keys that are stored in program memory. With the advent of the Trusted Computing (TC) technology, this hole has been patched and the TC uses both computer hardware and software to ensure proper behavior. DRMs were also developed to protect digital A/V content as it passed from device to device (e.g. DTCP).

IV. THE '236 PATENT

A. Overview

39. The '236 Patent is titled "Methods And Apparatuses For Secondary Conditional Access Server." As the cover shows, the application for the '236 Patent was filed on December 7, 2004.

40. As background to its alleged invention, the '236 Patent describes various aspects of conditional access (CA) and digital rights management (DRM) systems,

which were well-known to persons of ordinary skill in the art, as I have discussed above.¹ The '236 Patent then purports to disclose a method for “conditional access to media content of primary security systems on a secondary networked environment” and “bridging two security systems.”² Figure 2A, reproduced below, shows an example of a primary security system bridged to a secondary security system.³

¹ '236 Patent, 1:13-2:52.

² '236 Patent, Abstract, 2:56-59.

³ '236 Patent, 6:8-10.

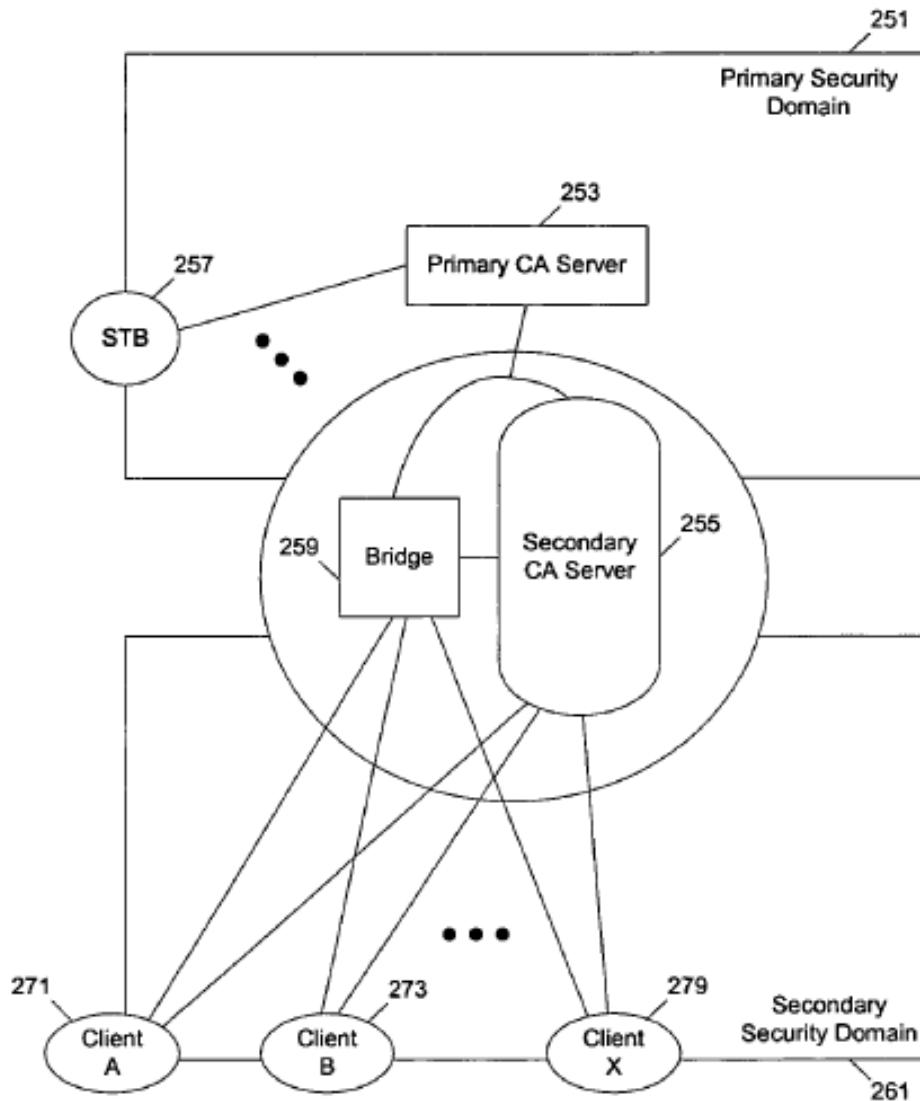


Fig. 2A

41. As shown in Figure 2A, a primary security domain 251 includes a primary CA server 253 in communication with a secondary CA server 255. Then, in a secondary security domain 261, secondary CA server 255 is in communication with a plurality of clients, including client 261. Since secondary CA server 256 is

in communication with primary CA server 253 in the primary security domain, and in communication with client 271 in the secondary security domain, “secondary CA server (255) bridges the primary security domain (251) and the secondary security domain (261).”⁴ The secondary CA server 255 acts as a client of the primary security domain and as a control information provider of the secondary security domain.⁵

42. In some embodiments, the primary security domain includes a broadcast CA system, and the secondary security domain includes a DRM system. In other embodiments, both security domains include CA systems. And in other embodiments, both security domains include DRM systems.⁶

B. Prosecution History of the '236 Patent

43. The application that issued as the '236 Patent was filed on December 7, 2004.⁷ During prosecution, the Examiner rejected the claims based on prior art, such as Grimes (U.S. 7,036,011), Candelore (U.S. 7,302,058), Simelius (U.S. 7,493,291), and Fransdonk (U.S. 6,961,858).⁸ According to the Examiner, the prior

⁴ '236 Patent, 7:8-43.

⁵ '236 Patent, 7:37-39.

⁶ '236 Patent, 2:61-3:16.

⁷ EX1002 (“'236FH”), 1-129.

⁸ '236FH, 296-324, 388-422, 506-541.

art showed it was known, for example, to configure a conditional access server with/as:⁹

- “one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain;”
- “a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the processor to process the security messages;”
- “the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages;” and
- “wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.”

44. In a later Amendment, the Patent Owner added to the claims terms of a “first security domain,” a “second security domain,” and a clause that “wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.”¹⁰

45. The Examiner later allowed the claims of the '236 Patent, stating that

⁹ '236FH, 470-471 (showing the language of claim 130 as of an amendment filed March 2, 2010), 509-513 (showing the Examiner's rejection of the pending claim 130).

¹⁰ '236FH, 594.

“Nowhere in the prior art is found, collectively, the *italicized* claim elements (i.e., ‘*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*’), at the time of the invention; serving to patentably distinguish the invention from said prior art.”¹¹ That is, the Examiner allowed the claims because they recited a substitution of a first security domain with a second security domain.

46. It is my understanding that the USPTO did not consider the Russ, Robert, or Eskicioglu prior art references, either alone or in combination as I discuss further below, during the original prosecution of the ’236 Patent.

V. LEVEL OF ORDINARY SKILL IN THE ART

47. In rendering the opinions set forth in this declaration, I was asked to consider the patent claims and the prior art through the eyes of a person having ordinary skill in the art at the time of the alleged invention. I understand that the factors considered in determining the ordinary level of skill in a field of art include the level of education and experience of persons working in the field; the types of problems encountered in the field, the teachings of the prior art, and the sophistication of the technology at the time of the alleged invention. I understand that a person having ordinary skill in the art is not a specific real individual, but

¹¹ ’236FH, 624.

rather is a hypothetical individual having the qualities reflected by the factors above. I understand that a person having ordinary skill in the art would also have knowledge from the teachings of the prior art, including the art cited below.

48. In my opinion, on or before February 11, 2009, a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer or electrical engineering, or a related field, and approximately two or more years of experience in computer and networking technology. Additional education could substitute for less professional experience, and vice versa. I believe I possess such experience and knowledge, and am qualified to opine on the '236 patent from the perspective of a person of ordinary skill in the art.

VI. CLAIM INTERPRETATION

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

49. Claims 32, 66, and 130 of the '236 Patent recite “access controlled data that is in an access controlled format and that is at least partially derived from the security messages.” In my opinion, this language does not require any particular interpretation beyond its ordinary and customary meaning in plain English. That is, the “access controlled data” “is in an access controlled format” and “is at least partially derived from the security messages.” The word “that” refers to the access controlled data.

50. I have been informed that the Patent Owner asserted infringement of this

limitation in district court, 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 showing the following figure:

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

EX1008, 17-18 (annotation in original).

51. In the event that Patent Owner is attempting to say the access controlled data's *format* is "partially derived from the security message," I disagree. The plain English reading of the limitation does not suggest this relationship, and I am not aware of any disclosures or examples in the '236 Patent that would support that understanding.

VII. OVERVIEW OF THE PRIOR ART

52. The following prior art references show that every element of the Challenged Claims was known in the art. Below, I provide a brief summary of these prior art references.

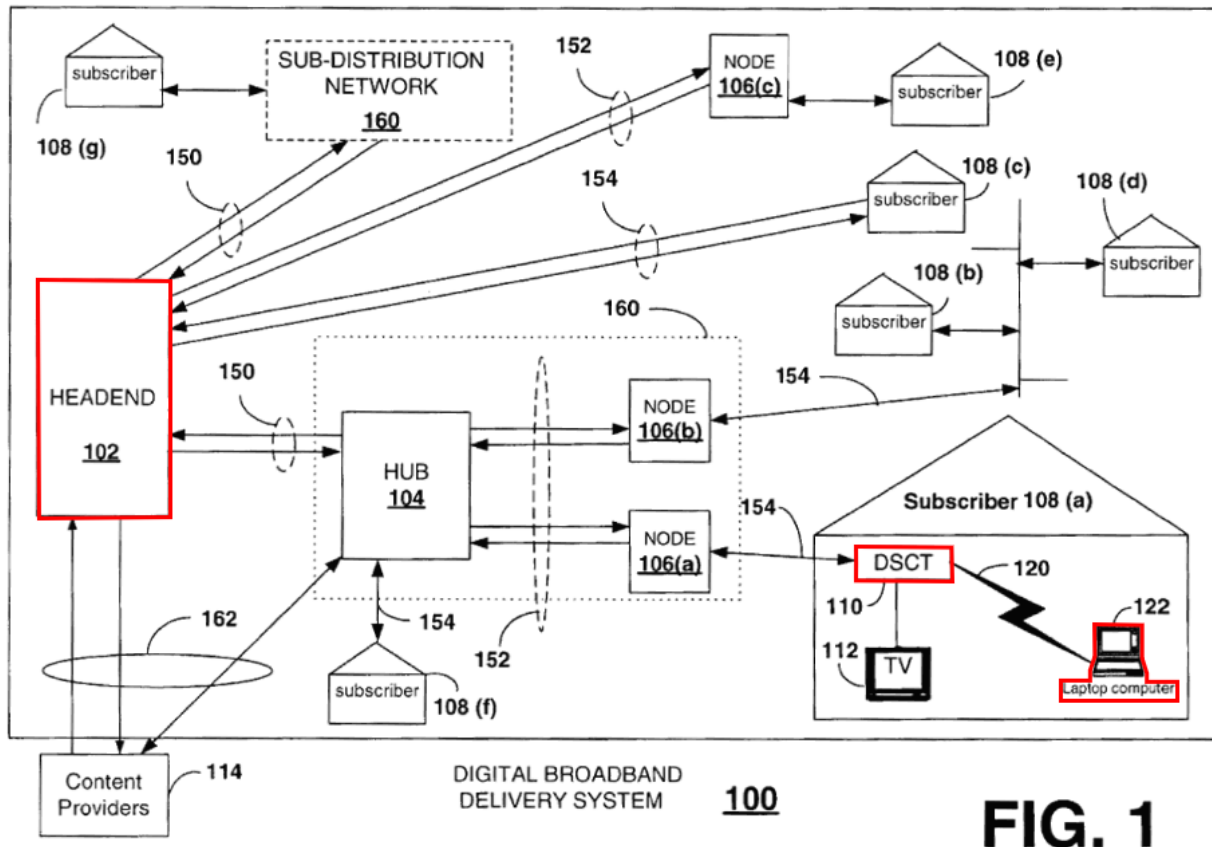
A. Russ

53. U.S. Patent No. 6,748,080 (EX1005; "Russ") is titled "Apparatus For Entitling Remote Client Devices," issued on June 8, 2004, and is based on U.S. patent application 10/154,495, filed on May 24, 2002. I have been informed that Russ qualifies as prior art to the '236 Patent.

54. Russ is directed to a "master-receiver in a subscriber television network [that] receives service instances and entitlement information from a headend of the subscriber television network and re-transmits service instances to a client-receiver after dynamic encryption scheme determination."¹² Service instances include, for example, audiovisual programs, Internet and telephone services, pay-per-view

¹² Russ, Abstract.

programming, and the like.¹³ An example of a digital broadband delivery system (DBDS) 100 according to Russ is shown in Figure 1, annotated below to highlight headend 102 and DSCT 110 and client-receiver 122 that are located in a subscriber location 108(a).



55. Headend 102 includes conditional access authority (CAA) logic “for controlling access to the DBDS” by enabling DSCT 110 to receive entitlements for service instances.¹⁴ In that regard, Russ discloses that DSCT 110 registers with the

¹³ Russ, 4:21-49, 13:5-9, 17:64-67, 20:7-11

¹⁴ Russ, 8:8-11, 10:48-50.

headend 102 and is entitled to service instances before receiving and accessing service instances.¹⁵ For example, headend 102 transmits secure messages to DSCT 110 including entitlement management messages (EMMs) that include entitlement information and entitlement control messages (ECMs) that include information for generating control words that decrypt or descramble protected service instances.¹⁶

56. At subscriber location 108, DSCT 110 manages a local network, to which client-receiver 122 joins.¹⁷ When client-receiver 122 joins DSCT 110's local network, client-receiver 122 identifies itself, and DSCT 110 determines an encryption scheme to use for communications with client-receiver 122.¹⁸ Russ identifies some examples of encryption schemes and protocols including secure sockets layer (SSL), Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CRPM), and transport layer security (TLS), but explains that any scheme or protocol known to persons of ordinary skill in the art may be used.¹⁹

57. At the subscriber location 108, DSCT 110 provides service instances and related entitlements to client-receiver 122, and "DSCT 110 acts as an entitlement

¹⁵ Russ, 7:56-58.

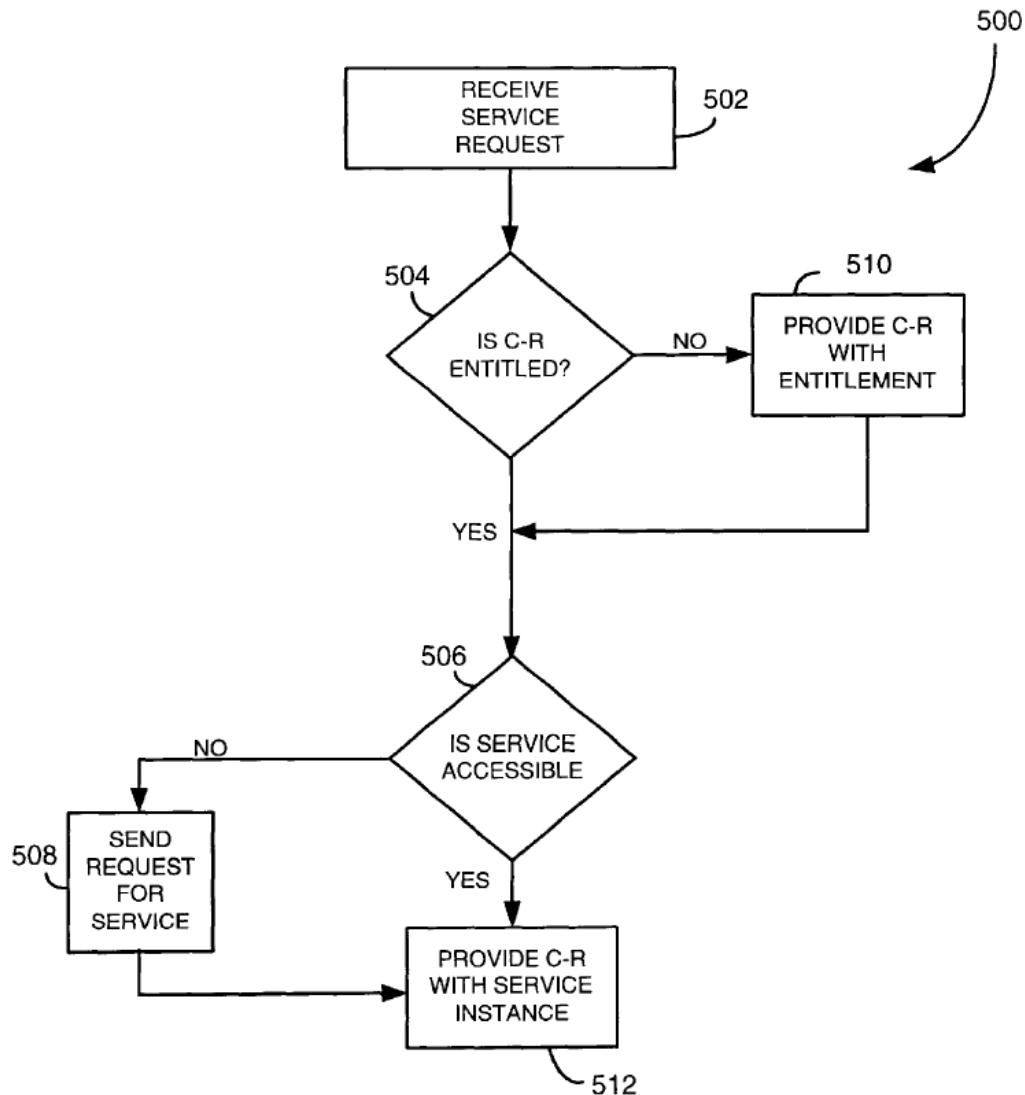
¹⁶ Russ, 8:4-37, 10:48-50, 12:14-17, 13:12-34.

¹⁷ Russ, 8:49-9:25, 16:32-42, 25:43-65.

¹⁸ Russ, 16:64-17:34.

¹⁹ Russ, 17:7-14.

granting authority for the client-receiver 122” and grants/deletes client-receiver 122’s entitlements to service instances based on information from headend 102.²⁰ Exemplary steps taken by DSCT 110 to service client-receiver 122 are shown in Figure 5 reproduced below.



²⁰ Russ, 17:61-18:40, 18:60-65.

FIG. 5

Steps include, for example:²¹

- Receiving a request for a service instance (step 502);
- Determining if client-receiver 122 is entitled to the service instance and then entitling client-receiver 122, which may include processing an entitlement received from headend 102 in an EMM (steps 504, 510);
- Determining if the service instance is available locally or requesting the service instance from headend 102 (steps 506, 508); and
- Providing the service instance to client-receiver 122 (step 512).

58. In receiving service instances from headend 102 and providing those service instances to client-receiver 122, DSCT 110 may be configured to first decrypt the service instance (for example using control words) and then re-encrypt the service instance “using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122” as discussed above.²²

²¹ Russ, 17:61-19:6.

²² Russ, 19:43-20:24, Fig. 6.

B. Robert

59. U.S. Patent No. 7,546,641 (EX1006; “Robert”) is titled “Conditional Access To Digital Rights Management Conversion,” issued on June 9, 2009, and is based on U.S. patent application 10/779,248, filed on February 13, 2004. I have been informed that Robert qualifies as prior art to the ’236 Patent.

60. Robert is directed to a system and method for interfacing between different content protection schemes, such as between conditional access (CA) and digital rights management (DRM) systems, “while maintaining security of the content and any associated protection information.”²³ Exemplary steps taken to interface CA and DRM systems are shown in Figure 5 reproduced below.

²³ Robert, Abstract, 2:23-33, 6:17-30.

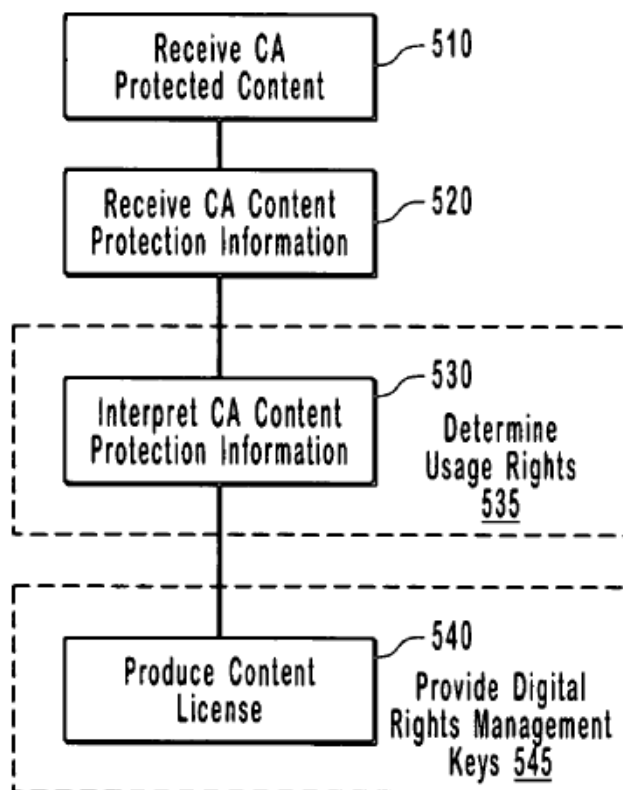


Fig. 5

Steps include, for example:²⁴

- Receiving CA protect content and CA content protection information (steps 510, 520);
- Interpreting the CA content protection information to determine usage rights, such as “how and under what conditions content may [be] consumed” (steps 530, 535); and
- Producing a content license and keys for enforcing digital rights at a

²⁴ Robert, 12:16-26.

device configured for DRM content protection scheme (steps 540, 545).

61. Within the broader steps outline above, Robert explains that there are a variety of ways for transcribing CA content for DRM systems. For example, CA control words can be included in a DRM license, CA encrypted content can be decrypted first before encrypting according to DRM methods, and transcription steps can be taken at any time or performed by different devices.²⁵

C. Eskicioglu

62. U.S. Patent No. 8,332,657 (EX1007; “Eskicioglu”) is titled “Global Copy Protection System For Digital Home Networks,” issued on December 11, 2012, and is based on U.S. patent application 09/936,415, filed on March 15, 2000, and further claims priority to several applications as listed on the cover page of Eskicioglu. I have been informed that Eskicioglu qualifies as prior art to the ’236 Patent.

63. Eskicioglu is directed to a system and method for “providing local security of audio and video content during transmission and storage within digital home networks” by rebundling keys required for descrambling into a “new ECM (LECM), which is protected by a local public key.”²⁶ An exemplary system

²⁵ Robert, 6:31-59.

²⁶ Eskicioglu, Abstract.

transmitting content from a source to a presentation device 16, such as a television, through an access device 14, such as a set-top box, is shown in Figure 1A reproduced below.²⁷

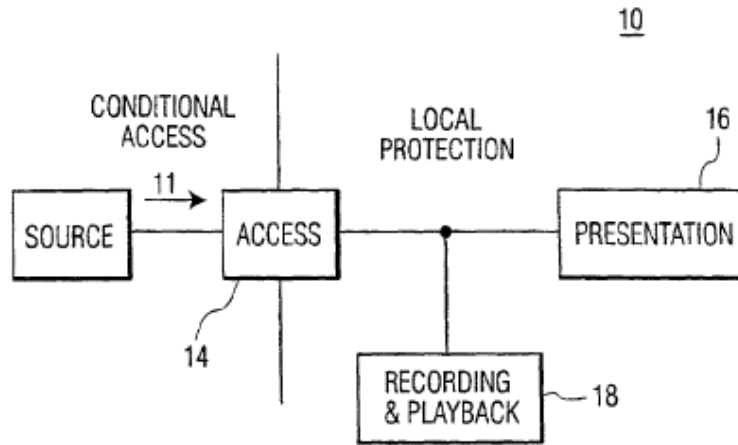


FIG. 1A

64. Describing the rebundling of an ECM into a local ECM (LECM), Eskicioglu states: “The encrypted descrambling key associated with the scrambled program is decrypted in the access device using a key associated with the service provider and then the key is re-encrypted using a public key associated with said access device. The presentation device decrypts the re-encrypted descrambling key and descrambles the scrambled data component using the descrambling key. This invention may also be utilized for managing access to a scrambled pre-recorded

²⁷ Eskicioglu, 3:13-21, 4:16-45.

program.”²⁸ Now protected by the LECM in the local network, and “[b]ecause every local network contains a unique set of public/private key pairs, only the local system which recorded or viewed the original content is capable of viewing any copies derived from its local network distributed content.”²⁹

D. Analogous Art

65. A person of ordinary skill in the art would have been aware of Russ, Robert, and Eskicioglu, and would have considered these prior art references to be in the same field as the '236 Patent. For example, the '236 Patent, Russ, Robert, and Eskicioglu are all directed towards content distribution and management, including protection. *See* '236 Patent, 1:5-2:53; Russ, Abstract, 1:5-2:14; Robert, Abstract, 1:12-2:19; Eskicioglu, 1:15-60.

VIII. GROUNDS OF UNPATENTABILITY

66. It is my opinion that the prior art references anticipate and/or render obvious the Challenged Claims of the '236 Patent as illustrated in the following Grounds:

²⁸ Eskicioglu, 2:20-29; *see also* Eskicioglu, 2:1-40, 7:41-53, 8:4-18.

²⁹ Eskicioglu, 8:10-16.

- **Ground 1:** Russ anticipates claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135;
- **Ground 2:** Russ renders obvious claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135;
- **Ground 3:** Russ in view of Robert renders obvious claims 35-36, 69-70, and 132-133;
- **Ground 4:** Russ in view of Eskicioglu renders obvious claims 40-41, 43, 74-75, 77, and 136-137.

67. In the sections that follow, I provide a detailed explanation of my opinion of how those prior art references show that the Challenged Claims are unpatentable.

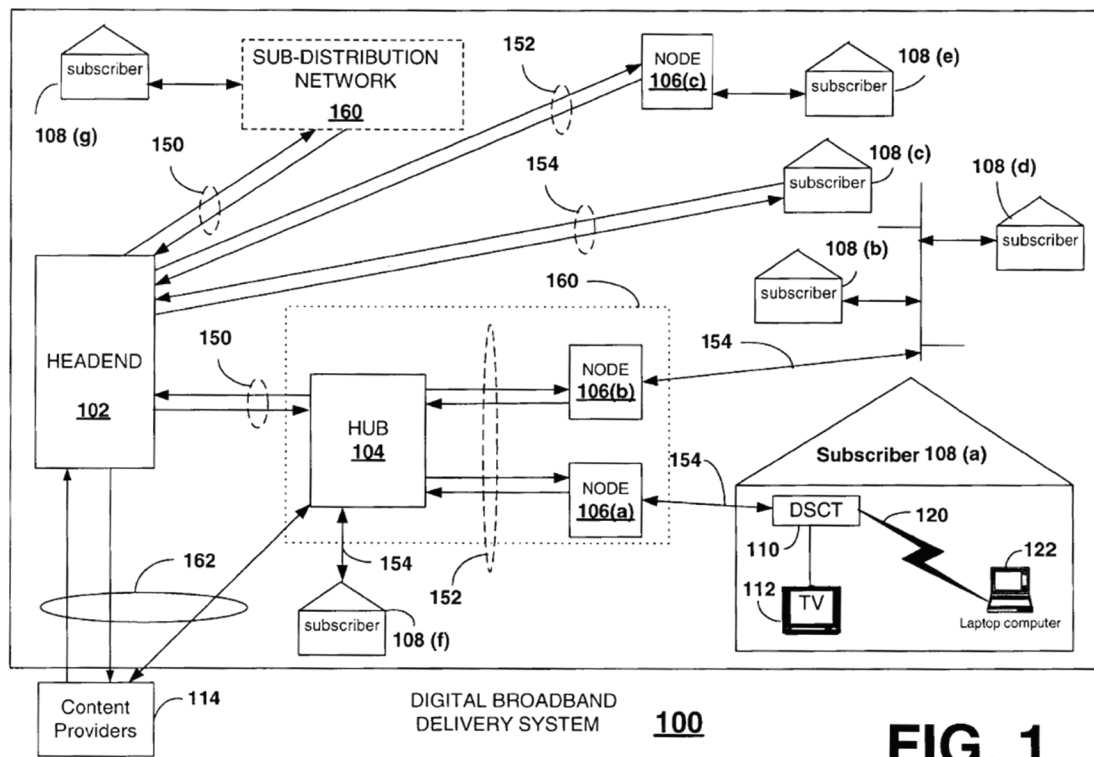
A. Ground 1: Russ anticipates claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135

1. Invalidity of claims 130-131 and 134-135

a. Claim 130[pre]

68. Claim 130[pre] recites “A conditional access server.” Russ discloses this preamble, whether it limits the claim or not.

69. Russ shows an example of a digital broadband distribution system (DBDS) 100 in Figure 1, reproduced below.



70. As shown, DBDS 100 includes DSCT 110 and client-receiver 122 (shown as a laptop in Figure 1) at subscriber location 108(a). DSCT 110 is conditional access server to client-receiver 122 because DSCT 110 serves client-receiver 122 with service instances (*i.e.*, content) and also “has the authority and capacity to grant and delete entitlements” for service instances to client-receiver 122.³⁰

71. For example, Figure 5, reproduced below, shows steps for DSCT 110 to

³⁰ Russ, 8:49-51, 17:61-18:51; *see also* Russ, 3:11-22, 4:21-39, 8:38-9:7, 19:7-42, 24:3-7, 24:37-38.

provide a service instance to a client-receiver.³¹

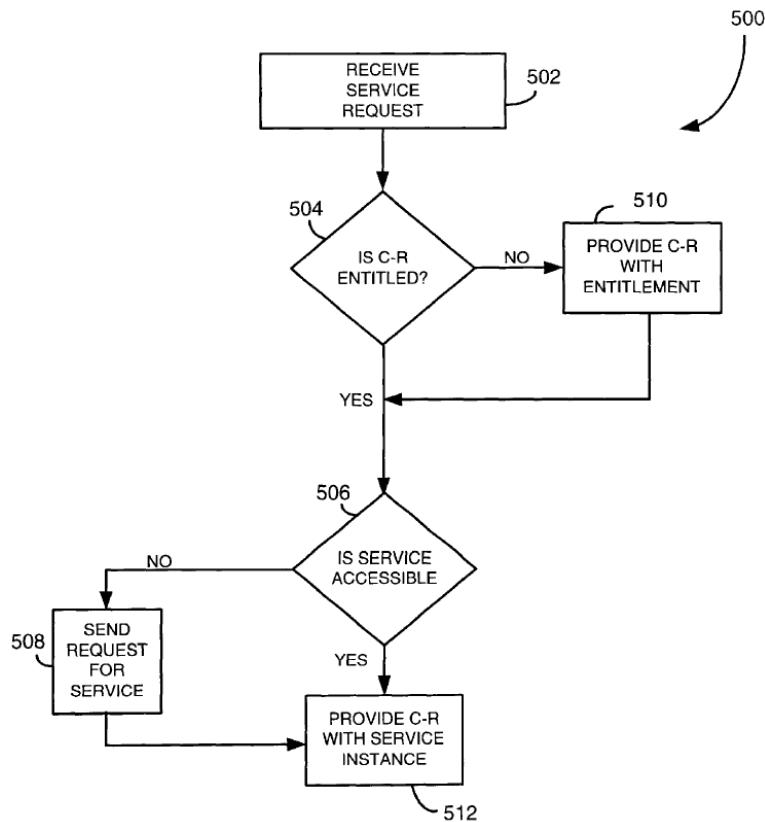


FIG. 5

These steps include:

- DSCT 110 receives a request from client-receiver 122 for a service instance (step 502);
- DSCT 110 providing client-receiver 122 with an entitlement for the selected service instance in an EMM (steps 504 and 510); and

³¹ Russ, 17:61-18:66.

- DSCT 110 providing the selected service instance to client-receiver 122 (step 512).

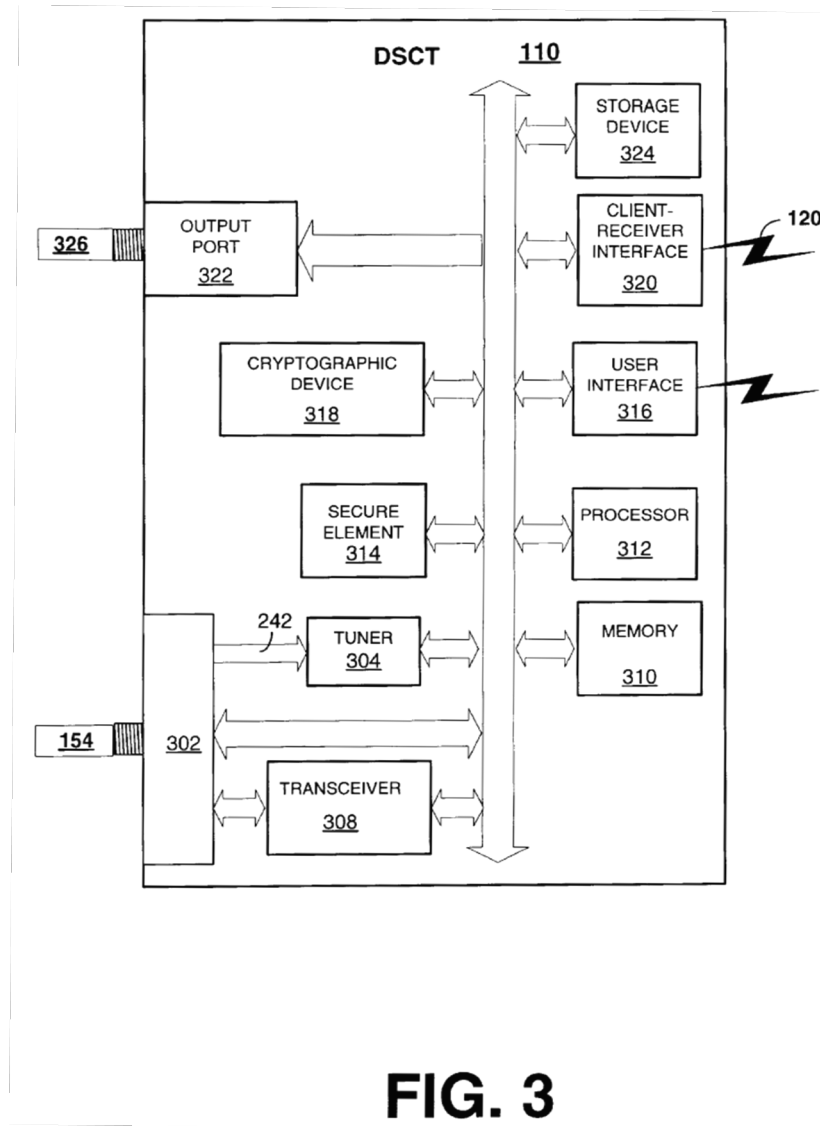
72. DSCT 110 is therefore a conditional access server, serving at least client-receiver 122.

73. Thus, Russ discloses a conditional access server, as claimed.

b. Claim 130[a]

74. **Claim 130[a] recites “one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain.”** Russ discloses this limitation.

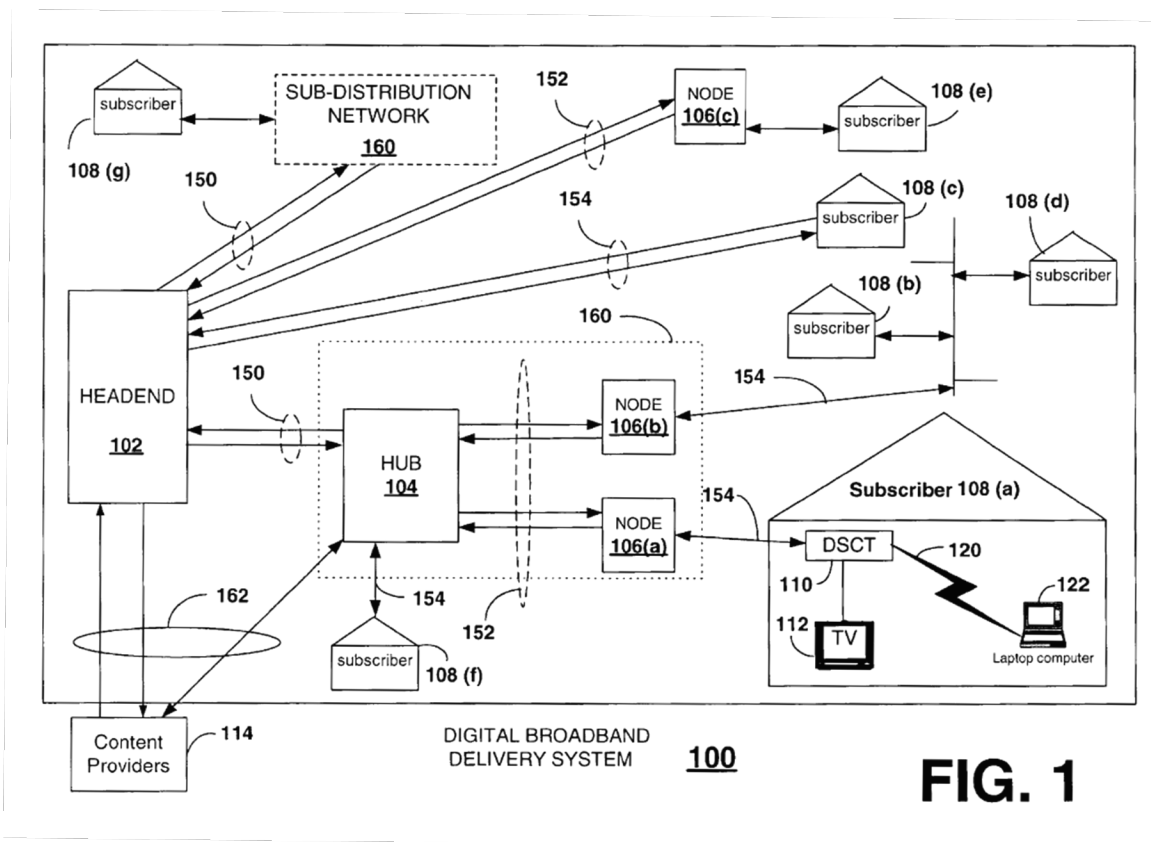
75. Russ shows an example of DSCT 110 in Figure 3, reproduced below. As shown, DSCT 110 includes several components for communication, such as input-output port 302, tuner 304, transceiver 308, client-receiver interface 320, and output port 322.



76. For example, Russ states that: “transceiver 308 receives out-of-band communication 258 from input port 302. The out-of-band communication data includes among other things system tables and messages including secure messages such as EMMs. EMMs are sent to the secure element 314 for processing

and the system tables are stored in memory 310.”³² The ’236 Patent describes an entitlement management message as one example of a security message.³³ Russ therefore discloses that DSCT 110 receives security messages at each of input port 302 and transceiver 308.

77. Russ further discloses that security messages, such as EMMs, are received from headend 102. Figure 1, reproduced below, shows headend 102 communicating with DSCT 110, either directly or through hub 104 and node 106.³⁴



³² Russ, 14:36-42; *see also* Russ, 7:7-20, 7:56-8:3, 10:39-56, 11:37-61, 13:53-56.

³³ ’236 Patent, 8:4-6, 40:46-47.

³⁴ Russ, 5:52-62.

78. DSCT 110 and headend 102 communicate securely with, for example, RSA encryption after having exchanged keys, after which DSCT 110 must register with headend 102 to be entitled to service instances.³⁵ In particular, headend 102 implements “conditional access authority (CAA) logic” for controlling access to the DBDS 100 and, for example, “send[ing] 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” and enabling DSCT 110 to receive entitlements for service instances.³⁶ Headend 102 therefore represents a primary security system in a first security domain because it implements measures to ensure secure communication with at least DSCT 110 and to ensure that service instances are only accessible to those entitled to them.

79. Thus, Russ discloses one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain, as claimed.

c. Claim 130[b.i]

80. **Claim 130[b.i] recites “a processor coupled to the one or more communication interfaces, the processor to process the security messages, and....”** Russ discloses this limitation.

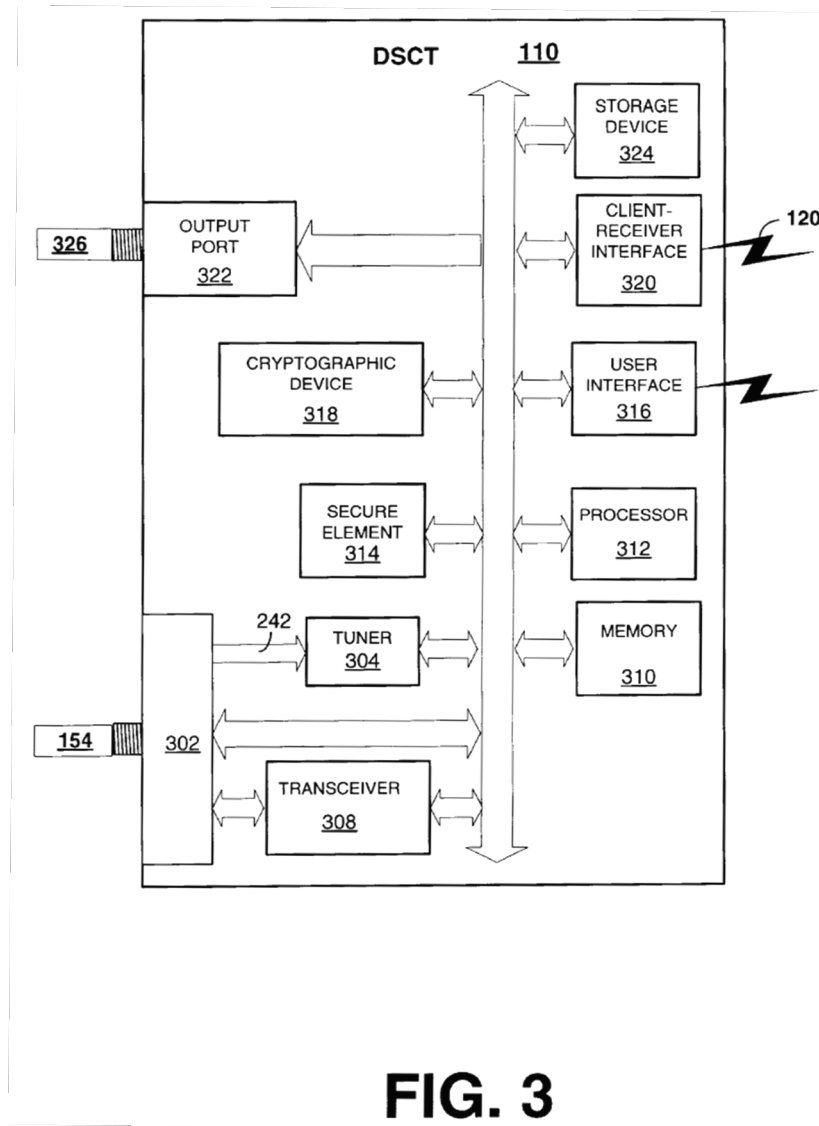
³⁵ Russ, 6:62-7:7, 7:56-58.

³⁶ Russ, 8:8-34, 10:48-65.

81. Russ shows an example of DSCT 110 in Figure 3, reproduced below. As shown, DSCT 110 includes a processor including secure element 314 and several components for communication, such as input-port 302 and transceiver 308, discussed above with respect to at least claim 130[a]. And, as shown, Figure 3 shows that secure element 314 communicates with input-port 302 and transceiver 308 through a common communication line or bus connecting the various components of DSCT 110.³⁷ For example, when transceiver 308 receives EMMs through input-port 302, the “EMMs are sent to the secure element 314 for processing.”³⁸

³⁷ Russ, 20:25-26.

³⁸ Russ, 14:36-42, 18:62-65.



82. An example of secure element 314 is further shown in Figure 7, reproduced below. Russ discloses that secure element 314 includes a processor 702 and entitlement management module 720 (or authorization/entitlement management module (AEMM)) that receives, authenticates, and implements EMMs.³⁹

³⁹ Russ, 21:11-21; *see also* 18:60-19:6, 22:40-23:67, 24:25-36.

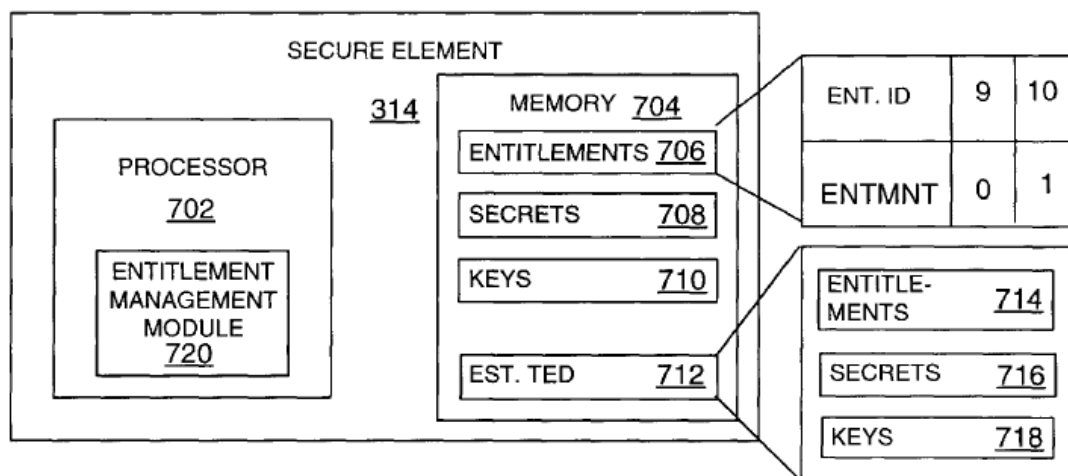


FIG. 7

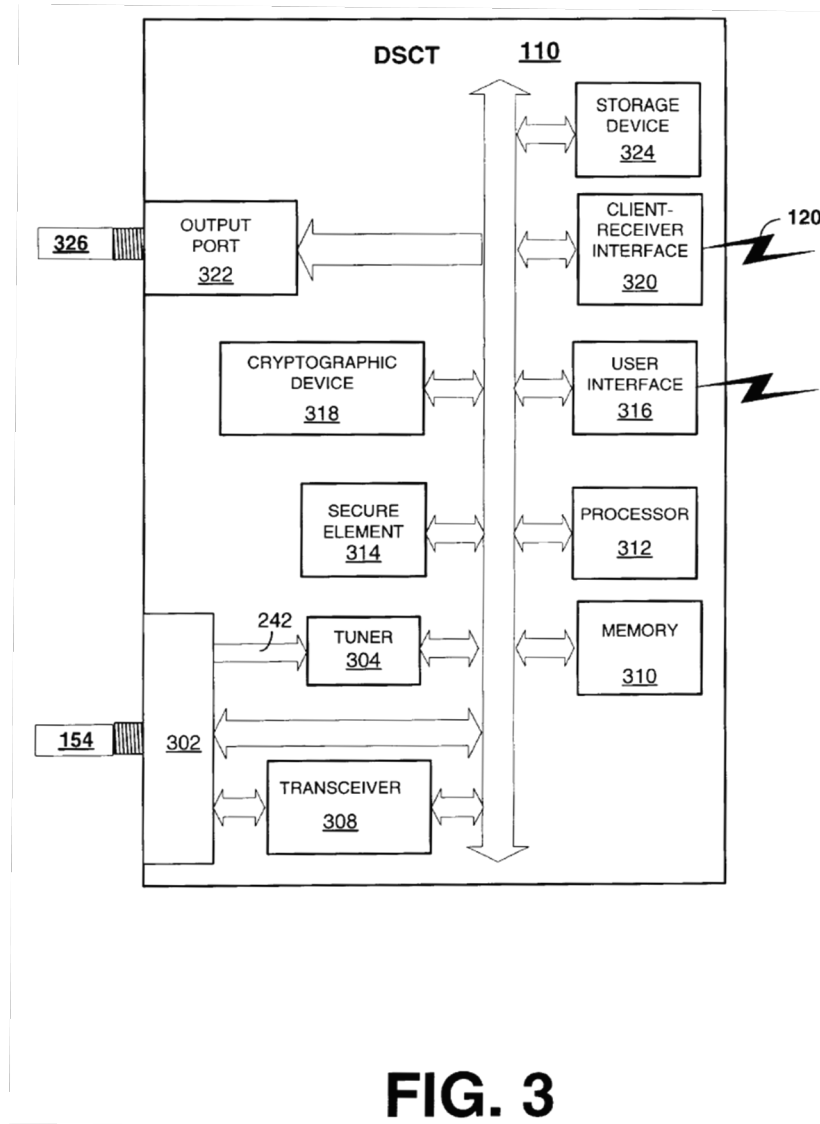
83. Thus, Russ discloses a processor coupled to the one or more communication interfaces, the processor to process the security messages, as claimed.

d. Claim 130[b.ii]

84. Claim 130[b.ii] recites “the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.” Russ discloses this limitation.

85. As I have discussed above with respect to at least claim 130[a] and as shown in Figure 3 reproduced below, Russ discloses that DSCT 110 includes a plurality of communication interfaces, including client-receiver interface 320, and output port 322. For example, communication link 120 interfacing DSCT’s client-receiver interface 320 may be a wired or wireless connection between client-receiver 122

and DSCT 110, such as an Ethernet connection or an IEEE 802.11 wireless standard.⁴⁰



86. When client-receiver 122 joins DSCT 110's network, DSCT 110 dynamically determines an encryption scheme to protect data communicated with

⁴⁰ Russ, 8:38-48, 13:53-65.

client-receiver 122.⁴¹ Figure 4, reproduced below, shows steps that DSCT 110 performs to determine an encryption scheme to use with client-receiver 122.⁴²

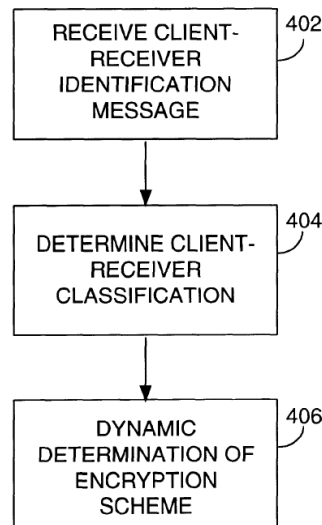


FIG. 4

Russ states that encryption may take the form of any scheme or protocol known to a person of ordinary skill in the art, including “secure sockets layer (SSL) protocol, Digital Transmission Content Protection (DTCP), Content Protection for Recordable Media (CPRM), and transport layer security (TLS) protocol.”⁴³ Indeed, a person of ordinary skill in the art would have been familiar with all those listed and more.

⁴¹ Russ, 9:9-12, 16:64-17:14.

⁴² Russ, 17:15-34.

⁴³ Russ, 17:7-14.

87. DSCT 110 will then use the determined encryption scheme—DTCP, for example—during communications with client-receiver 122 “to protect the privacy of the communication.”⁴⁴ For example, Russ states that service instances are encrypted “using [the] encryption scheme that was dynamically negotiated by the DSCT 110 and the client receiver 122.”⁴⁵ Content of EMMs communicated from DSCT 110 to client-receiver 122 are also encrypted.⁴⁶ Russ therefore discloses transmitting, from DSCT 110 to client-receiver 122, service instances and EMMs in an encrypted format dynamically determined between DSCT 110 and client-receiver 122, such as according to DTCP protocols.

88. Russ further discloses that service instances and EMMs transmitted from DSCT 110 to client-receiver 122 are derived from security messages transmitted from headend 102 to DSCT 110 (*e.g.*, EMMs transmitted from headend 102 to DSCT 110). For example, DSCT 110 is first entitled to a service instance through an EMM from headend 102 before it decrypts the service instance and re-encrypts it for transmission to client-receiver 122 using the determined encryption scheme.⁴⁷ And, for a particular requested service instance, an entitlement generator 236 in

⁴⁴ Russ, 16:64-17:14.

⁴⁵ Russ, Fig. 6, 20:14-24; *see also* Russ, 21:11-21.

⁴⁶ Russ, 21:22-65, 24:1-24.

⁴⁷ Russ, 8:8-34, 15:46-52.

headend provides an entitlement to DSCT 110 in an EMM, and DSCT 110 processes the received EMM and provides an entitlement to client-receiver 122 in an EMM.⁴⁸ Russ therefore discloses that both service instances and EMMs are access controlled data at least partially derived from the security messages.

89. Russ’s disclosures above indicate that DSCT 110 and client-receiver 122 function together in a second security domain, as claimed. Particularly, DSCT 110 and client-receiver 122 communicate in the local network at subscriber location 108 and using an encryption scheme specifically determined between the two (for example, DTCP)—and one not used between headend 102 and any other component. Moreover, the communications are secured via shared secrets between DSCT 110 and client-receiver 122.⁴⁹

90. Thus, Russ discloses that the one or more communication interfaces transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages, as claimed.

91. Additionally, as I discussed above in Section VI.A, it is my understanding that the Patent Owner may be arguing that this claim limitation’s “access controlled data” has a format that is “partially derived from the security message.”

⁴⁸ Russ, 18:52-65, 24:1-24.

⁴⁹ Russ, 20:25-53.

Russ discloses this as well. For example, Russ states that headend 102 may send DSCT 110 an EMM to instruct DSCT 110 which encryption scheme it is supposed to use in its communication with client-receiver 122.⁵⁰ Therefore, Russ discloses partially deriving an access controlled format from an EMM.

92. Thus, Russ discloses, in an additional way, that the one or more communication interfaces transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages, as claimed.

e. Claim 130[c.i]

93. Claim 130[c.i] recites “wherein the primary security system authenticates the conditional access server clients of the primary security system through a first authentication process using a first root of trust and....” Russ discloses this limitation.

94. Russ discloses that headend 102 authenticates DSCT 110. As Russ explains, each DSCT 110 is manufactured with a unique serial number and a private key-public key pair, which are provided to operator of the DBDS 100—headend 102.⁵¹ When DSCT 110 registers with headend 102, which it must do before receiving

⁵⁰ Russ, 25:17-22; *see also* Russ, 16:31-63, 19:7-27, 25:22-25.

⁵¹ Russ, 7:21-39, 8:4-11.

entitlements and service instances, DSCT 110 sends its serial number to headend 102, which registers DSCT 110 if the serial number matches a serial number in its database.⁵² DSCT 110 is provided with a trusted public key for use.⁵³

95. Russ therefore discloses that headend 102 authenticates DSCT 110 using a first root of trust based on the fact that DSCT 110 is manufactured with a unique serial number and keys. As Russ states, “the manufacturer is a key certification authority” that is implicitly trusted.⁵⁴ A person of ordinary skill in the art would have recognized that a root of trust is therefore established at initial programming time for DSCT 110 and its secure element. To elaborate on such a process, the secure element would have been programmed, for example, with keys of three manufacturer Conditional Access Authorities (CAAs) in a secure facility. The CAA keys are public/private key pairs, preferably RSA keys. Within the facility, unprogrammed secure elements are fed by spool into a programming station that writes the three manufacturer CAAs into the memory of each secure element and then the ability for the secure element to be programmed is turned off. At this point, the keys are implicitly trusted. The secure elements are then embedded into DSCTs. When DSCTs are to be sent to specific network operators, the CAA of the

⁵² Russ, 7:56-66.

⁵³ Russ, 7:58-66.

⁵⁴ Russ, 7:40-55.

network operator replaces one of the manufacturer CAAs with the CAA of the network operator via messages signed with the trusted keys of two of the CAAs. From that point on, the DSCT will trust messages signed by the network operator CAA. Such messages are made, for example, by entitlement generator 236. The DSCT and its secure element therefore have a root of trust established since manufacture.

96. Thus, Russ discloses that the primary security system authenticates the conditional access server clients of the primary security system through a first authentication process using a first root of trust, as claimed.

f. Claim 130[c.ii]

97. **Claim 130[c.ii] recites “the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and....”** Russ discloses this limitation.

98. Russ discloses that DSCT 110 authenticates client-receiver 122. As discussed with respect to at least claim 130[b.ii] above, DSCT 110 communicates with client-receiver 122 using an encryption scheme determined specifically for use between DSCT 110 and client-receiver 122, and one such determination is to

use DTCP protocols.

99. DTCP protocols require that devices undergo a handshaking process, known as an Authentication and Key Exchange (AKE), before protected communications are to take place. A person of ordinary skill in the art would have been familiar with such processes—and, indeed, authentication was a feature generally used in content protection systems as an additional layer of security. For example, DTCP's AKE was a recognized function for preventing illegal copying and identifying devices deemed safe in advance.^{55,56}

A representative example of such a mechanism is DTCP (Digital Transmission Contents Protection) of the IEEE 1394. **This mechanism prevents the eavesdropping by the third party by carrying out the authentication and key exchange procedure between a transmitting device and a receiving device of the AV data on the IEEE 1394 so as to share an encryption key for encrypting or decrypting the AV data, and transferring the AV data on the IEEE 1394 after encrypting the AV data by using this encryption key. This mechanism also incorporates a mechanism for preventing the illegal copy by an illegal receiving device by permitting the above described authentication and the key exchange (more specifically, the exchange of Certificate) only between those devices for which the safety is guaranteed in advance.**

100. The DTCP certificate identifies a DTCP device and contains verifiable proof

⁵⁵ U.S. Patent Application Publication No. 2002/0025042 (EX1010), [0009].

⁵⁶ *See also* U.S. Patent Application Publication No. 2003/0078891 (EX1012), [0041].

that the device is licensed to operate as a DTCP device.⁵⁷ Licensing in this case is performed by a trusted licensing authority, such as the Digital Transmission Licensing Administrator (“DTLA”), which is the licensing organization of DTCP.⁵⁸

101. Russ therefore discloses that DSCT 110 authenticates client-receiver 122, for example via a DTCP AKE, which is based on a certificate issued by a trusted authority, such as the DTLA. Because DSCT 110 and client-receiver utilize DTCP authentication based on a root of trust established by DTCP/DTLA protocols and certificates, and because headend 102 is not disclosed as using any DTCP-related protocols with respect to DSCT 110, the authentication between DSCT 110 and client-receiver 122 is independent and different from that between headend 102 and DSCT 110, as I have discussed with respect to claim 130[c.i] above.

102. Thus, Russ discloses that the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, as claimed.

⁵⁷ U.S. Patent Application Publication No. 2005/0027984 (EX1011), [0053].

⁵⁸ EX1011, [0107].

g. Claim 130[c.iii]

103. Claim 130[c.iii] recites “wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.” Russ discloses this limitation.

104. Russ discloses that service instances received at DSCT 110 are already encrypted by keys, for example by control words⁵⁹ that can be obtained by using a multi-session key (MSK) to encrypt a particular counter value.⁶⁰ Headend 102 provides DSCT 110 with MSKs and counter values in EMMs and ECMs so that it has the necessary information to decrypt service instances.⁶¹

105. Russ discloses that DSCT 110 decrypts data received from headend 102 and then re-encrypts that data for communication to client-receiver 122. Figure 6, reproduced below, shows an example of DSCT 110 providing a service instance to client-receiver 122.

⁵⁹ The '236 Patent Background includes some discussion of control words. *See* '236 Patent, 1:13-40.

⁶⁰ Russ, 13:14-34.

⁶¹ Russ, 11:37-46, 13:14-34.

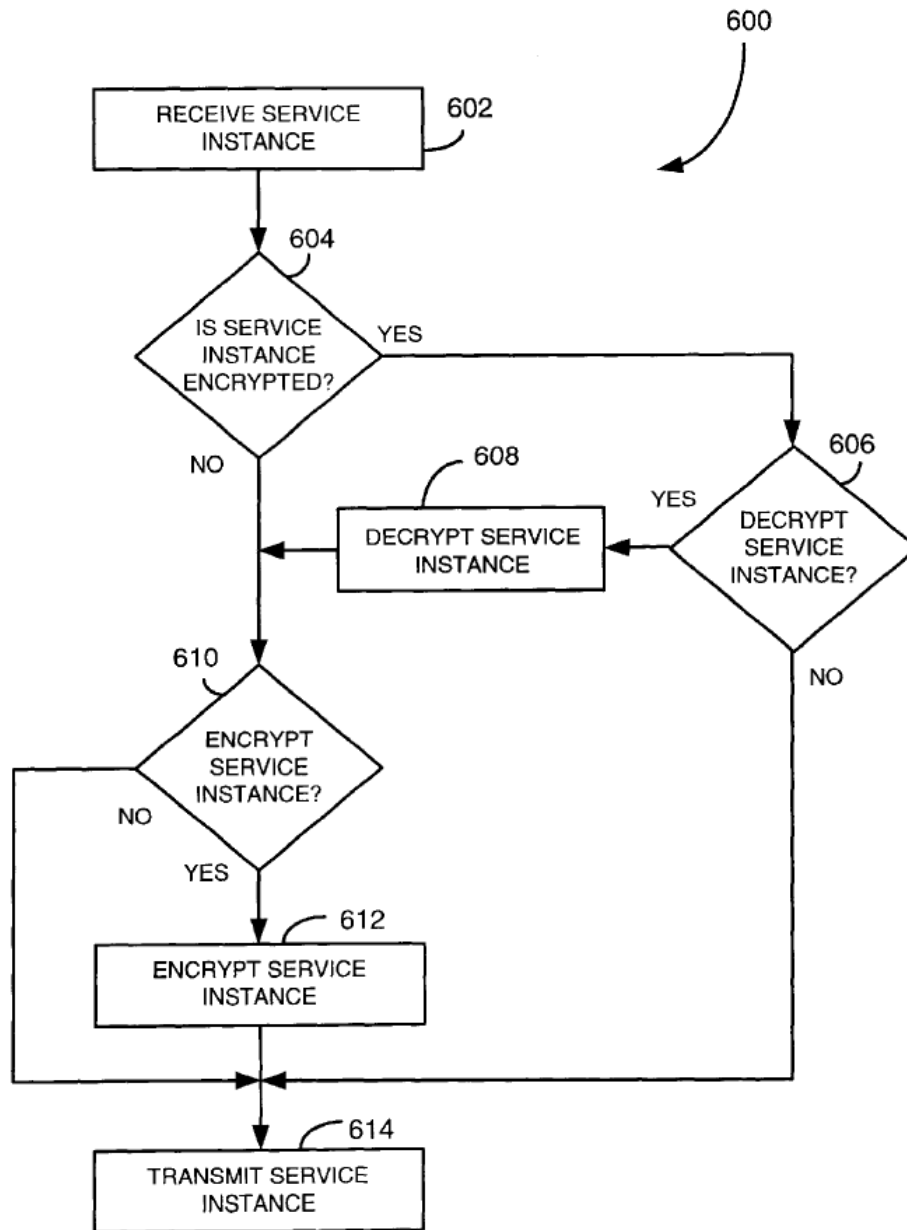


FIG. 6

Steps performed by DSCT 110 include,⁶² for example:

⁶² Russ, 19:52-20:19.

- Receiving a service instance from headend 102 or retrieving a service instance from storage (step 602);
- Decrypting the service instance with control words (step 608);
- Encrypting the service instance “using an encryption scheme that was dynamically negotiated by the DSCT 110 and the client-receiver 122” (step 612); and
- Transmitting the service instance to client-receiver 122.

106. As I discussed above with respect to at least claim 130[b.ii], the “encryption scheme ... dynamically negotiated by the DSCT 110 and the client-receiver 122” referenced in step 612 immediately above uses, in one example, DTCP protocols.

107. Russ therefore discloses that DSCT 110 substitutes the first security domain, which is the domain created by headend 102 in communicating with DSCT 110, with the second security domain, which is the domain created by DSCT 110 in communicating with client-receiver 122, for communications it has with client-receiver 122.

108. Thus, Russ discloses that the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust, as claimed.

h. Claim 131

109. Claim 131 recites “The conditional access server of claim 130, wherein

the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system.”

Russ discloses this limitation.

110. As I have discussed with respect to at least claims 130[a] and 130[b.ii] above, Russ discloses that DSCT 110 receives security messages such as entitlement management messages (EMMs).⁶³

111. And, as I have discussed with respect to at least claims 130[b.ii] and 130[c.ii] above, Russ discloses that between DSCT 110 and client-receiver 122, access controlled data is protected using DTCP protocols.⁶⁴ A person of ordinary skill in the art would have recognized DTCP as a form of digital rights management. For example, DTCP is considered an example of the “oldest DRM system ... known as CCI.”⁶⁵

112. Thus, Russ discloses that the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system, as claimed.

i. Claim 134[pre]

113. Claim 134[pre] recites “The conditional access server of claim 131,

⁶³ See Russ, 8:4-37, 10:48-65, 25:17-25.

⁶⁴ See Russ, 8:4-37, 10:48-65, 25:17-25.

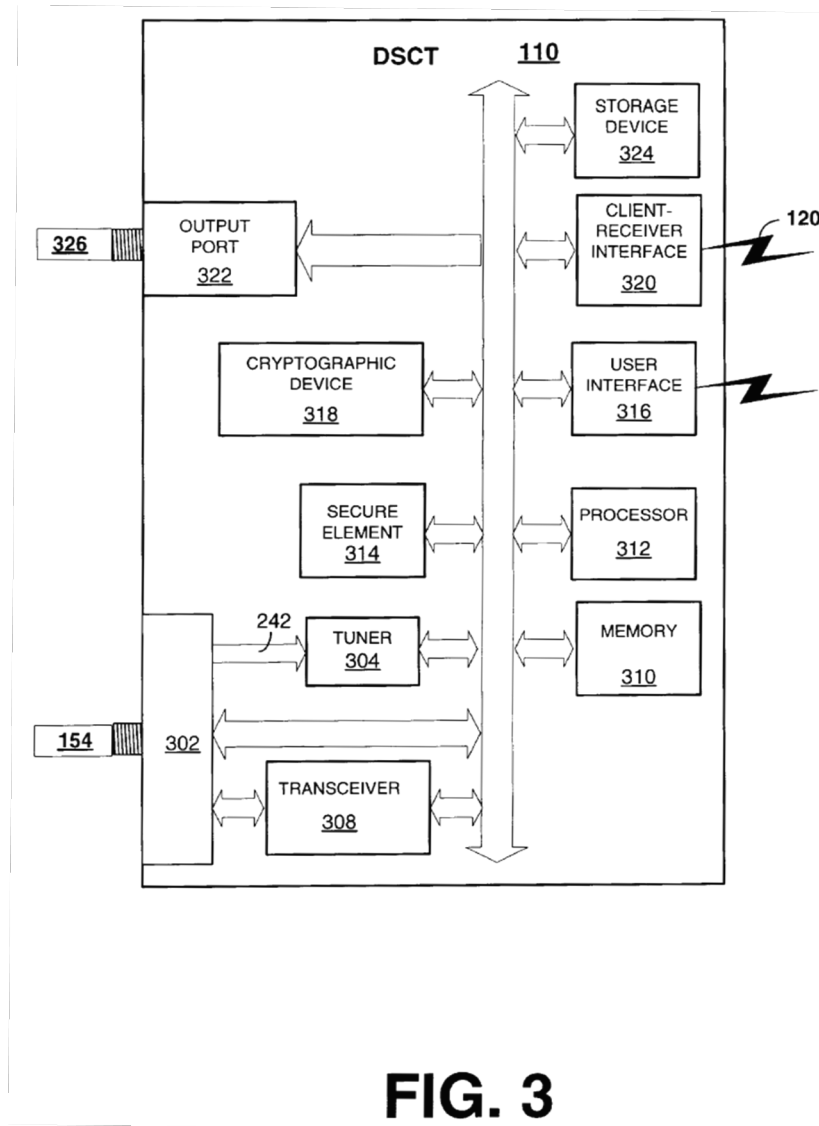
⁶⁵ EX1012, [0041]. See also U.S. Patent Application Publication No. 2004/0098583 (EX1013), [0014].

wherein....” Russ discloses the conditional access server of claim 131, as I have discussed above.

j. Claim 134[a]

114. Claim 134[a] recites “the one or more communication interfaces are to receive an entitlement control message and scrambled content of the primary security system; and the conditional access server further comprises....” Russ discloses this limitation.

115. As I have discussed above with respect to at least claim 130[a], and as shown in Figure 3 reproduced below, Russ discloses that DSCT 110 includes a plurality of communication interfaces, including input-port 302 and tuner 304.



116. Russ further discloses receiving, through input-port 302 and tuner 304, “in-band communication”, such as transport stream 242.⁶⁶ Headend 102 generates transport stream 242 using multi-transport stream receiver-transmitter 228, which is shown in Figure 2, reproduced below.

⁶⁶ Russ, 15:1-6.

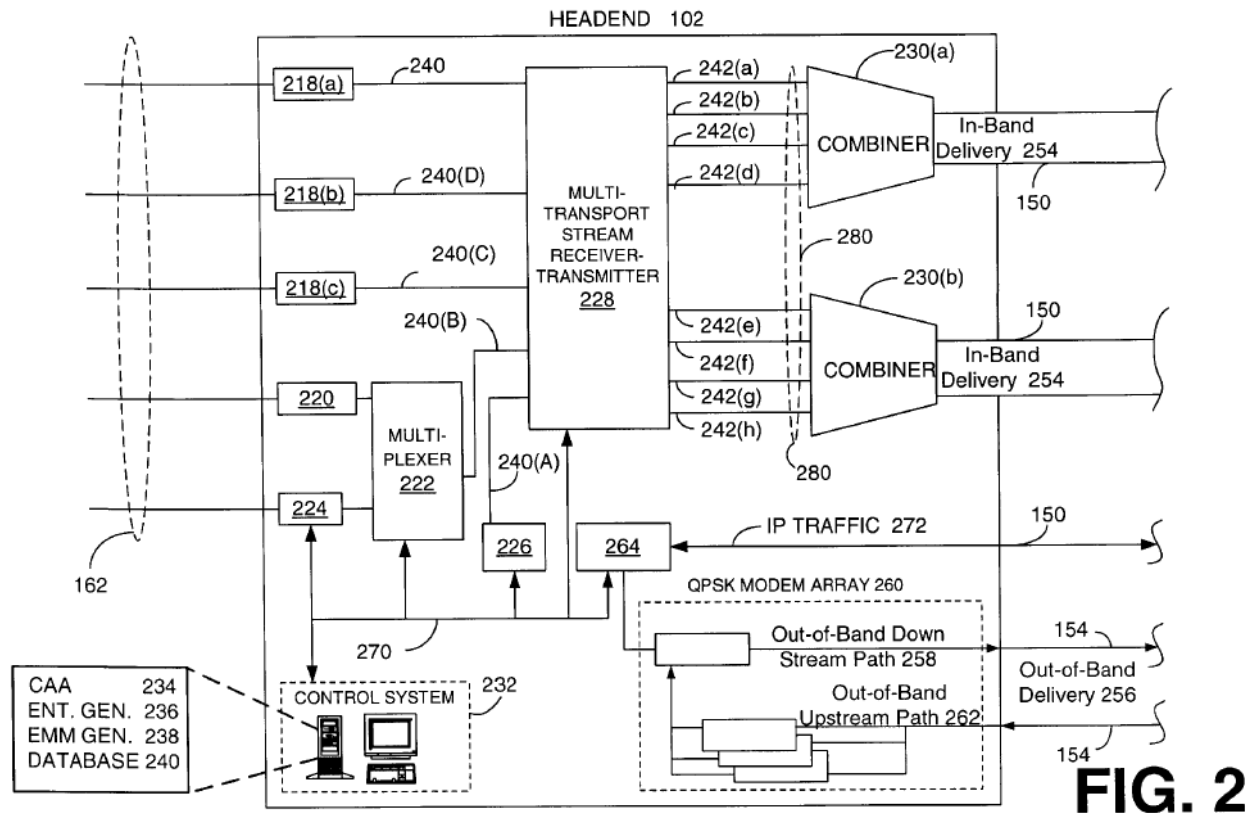


FIG. 2

117. Russ discloses that “multi-transport stream receiver-transmitter 228 is adapted to encrypt content,” for example using DES, DVB Common Scrambling, and/or other techniques such as those using the MSK and control words discussed above, “prior to modulating and transmitting the content.”⁶⁷ Furthermore, the output transport stream 242 includes an entitlement control message (ECM) including the counter value used to generate control words.⁶⁸ Russ therefore discloses DSCT 110 receiving an ECM and an encrypted service instance from headend 102.

⁶⁷ Russ, 12:47-13:19.

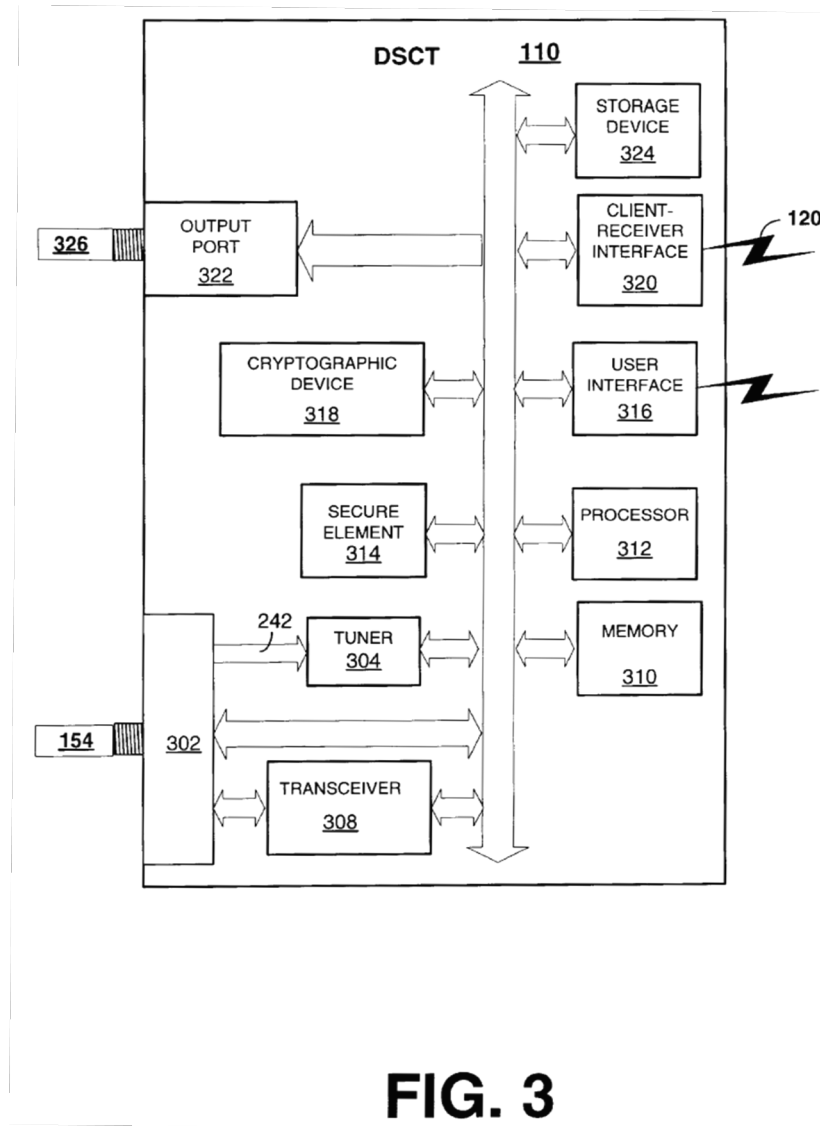
⁶⁸ Russ, 13:20-23; *see also* Russ, 13:3-5.

118. Thus, Russ discloses that the one or more communication interfaces are to receive an entitlement control message and scrambled content of the primary security system, as claimed.

k. Claim 134[b]

119. Claim 134[b] recites “a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message.” Russ discloses this limitation.

120. Russ discloses that DSCT 110 includes cryptographic device 318, coupled to secure element 314, for performing cryptographic functions. *See* Figure 3, reproduced below.



121. Russ discloses that cryptographic device 318 decrypts encrypted service instances according to the ECM. For example, the ECM includes a counter value that is used to generate a control word used to decrypt the service instance, and secure element 314 provides the control word to cryptographic device 318 to

decrypt the service instance.⁶⁹ Additionally, the ECM also includes an entitlement specifier, which DSCT 110 uses to determine whether it is entitled to service instances.⁷⁰

122. Finally, when “DSCT 110 is entitled to the selected service instance, the secure element 314 provides the cryptographic device 318 with the control word used for decrypting the selected service instance,” and “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.”⁷¹

Russ therefore discloses that DSCT 110 includes cryptographic device 318, which is communicatively coupled to secure element 314, for decrypting service instances according to the received ECM specifying both DSCT 110’s rights to the service instance and a counter value used to decrypt the service instance.

123. Thus, Russ discloses a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message, as claimed.

I. Claim 134[c]

124. Claim 134[c] recites “wherein the access controlled data comprises a

⁶⁹ Russ, 13:12-34, 23:60-67.

⁷⁰ Russ, 13:35-39, 23:25-46.

⁷¹ Russ, 15:46-54.

result of descrambling the scrambled content.” Russ discloses this limitation.

125. As I discussed with respect to at least claims 130[b.ii], 130[c.iii], and 134[b] above, Russ discloses descrambling (or decrypting) the encrypted service instance and then encrypting the decrypted service instance for transmission to client-receiver 122 using the encryption scheme negotiated between DSCT 110 and client-receiver 122. Russ therefore discloses that the service instance transmitted to client-receiver 122, protected under DTCP protocols, for example, includes the result of decrypting the service instance that was originally encrypted by headend 102.

126. Thus, Russ discloses that the access controlled data comprises a result of descrambling the scrambled content, as claimed.

m. Claim 135[pre]

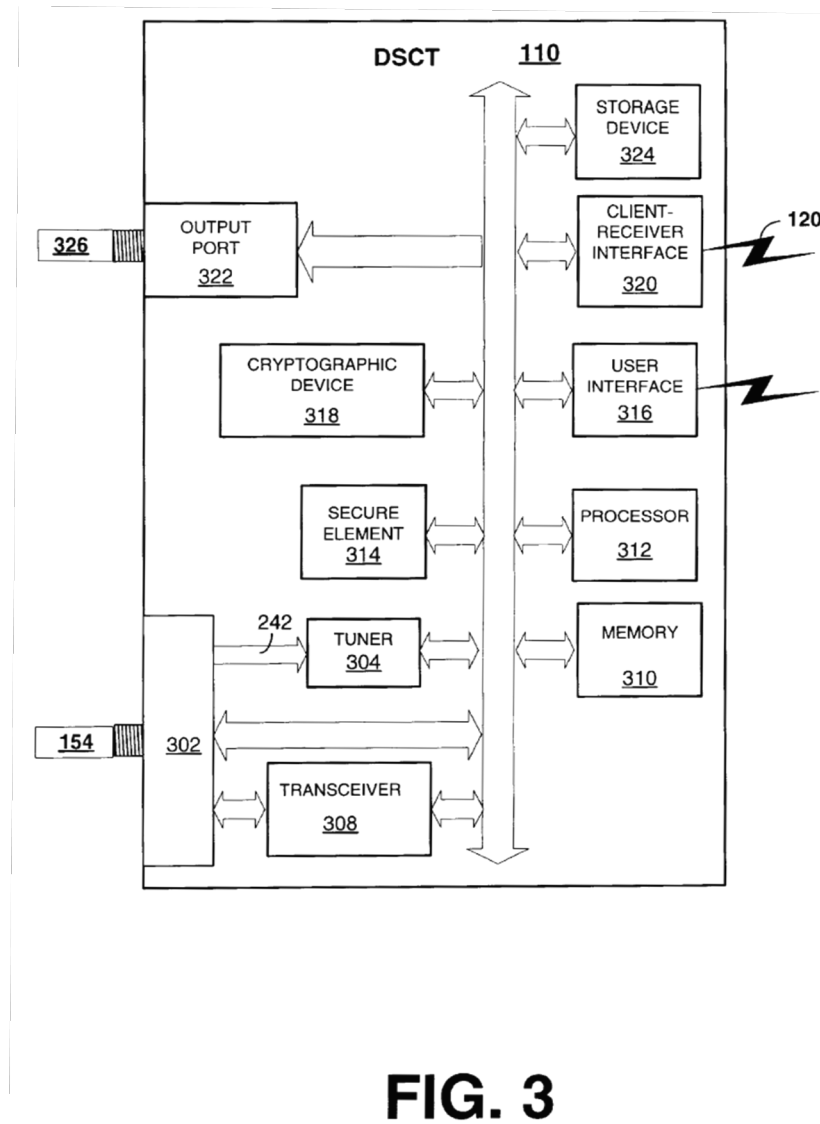
127. Claim 135[pre] recites “**The conditional access server of claim 134, further comprising....**” Russ discloses the conditional access server of claim 134, as I have discussed above.

n. Claim 135[a]

128. Claim 135[a] recites “**a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form.**” Russ discloses this limitation.

129. Russ discloses that DSCT 110 includes storage device 324 that, as shown in

Figure 3 reproduced below, is connected to DSCT 110's various input and output interfaces such as input-port 302, tuner 304, transceiver 308, client-receiver interface 320, and output port 322.



130. Storage device 324 is “for storing service instances” and may be configured as an external storage connected via output-port 322 or some other input/output

interface.⁷² DSCT 110 stores service instances in storage 324 so that they may be retrieved when requested by client-receiver 122.⁷³ Service instances from headend 102 may be stored encrypted or not encrypted, and so DSCT 110 checks whether requested service instances are encrypted and whether they require decryption before further processing for transmission to client-receiver 122.⁷⁴

131. Thus, Russ discloses a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form, as claimed.

o. Claim 135[b]

132. Claim 135[b] recites “wherein the access controlled data is provided in response to a request from the secondary conditional access client.” Russ discloses this limitation.

133. Russ discloses that DSCT 110 provides EMMs, which include entitlements to service instances, and service instances to client-receiver 122 in response to “a request from the client-receiver 122 for a service instance.”⁷⁵ Russ shows this in Figure 5, reproduced below, showing DSCT 110 receiving a request from client-

⁷² Russ, 15:55-62.

⁷³ Russ, 19:35-39, 19:45-54.

⁷⁴ Russ, 15:16-26, 19:45-54, Fig. 6.

⁷⁵ Russ, 17:61-18:66.

receiver 122 for a service instance (step 502), providing client-receiver 122 with an entitlement via an EMM (step 510), and providing client-receiver 122 with a service instance (step 512).

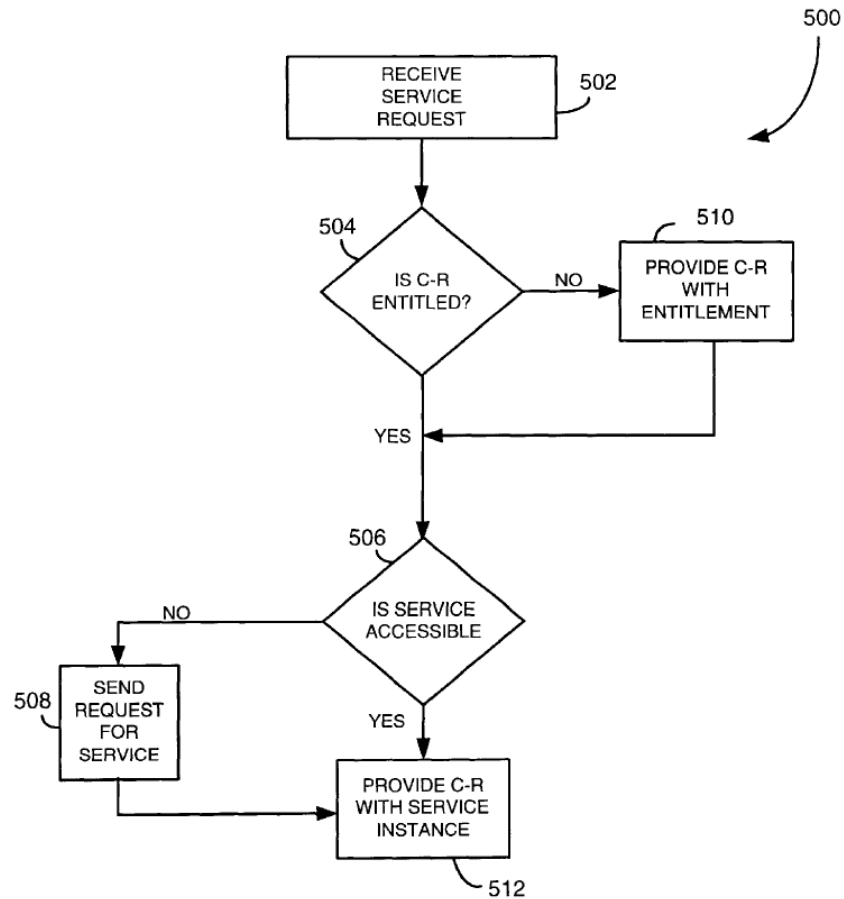


FIG. 5

134. Thus, Russ discloses that the access controlled data is provided in response to a request from the secondary conditional access client, as claimed.

2. Invalidity of claims 32-34 and 38-39

135. Independent claim 32 is directed to “A method to process conditional access protection,” while independent claim 130 discussed above is directed to “A conditional access server.” Nevertheless, their limitations are substantially the same and therefore disclosed by the prior art for the same reasons. Below, I reference the relevant claim limitations of claim 130 and its dependent claims that disclose the same subject matter, and/or supplement with additional disclosures where limitations may differ.

a. Claim 32[pre]

136. Claim 32[pre] recites “A method to process conditional access protection, the method comprising...” Russ discloses this limitation.

137. As I have discussed with respect to claim 130 above, Russ discloses that DSCT 110, along with headend 102 and client-receiver 122, processes conditional access protection for service instances by, for example, entitling client-receiver 122 to service instances and providing service instances to client-receiver 122.

138. Thus, Russ discloses a method to process conditional access protection.

b. Claim 32[a]

139. Claim 32[a] recites “receiving, at a conditional access server, security messages of a primary security system in a first security domain.” Russ discloses this limitation, as I have discussed with respect to at least claims 130[pre]

and 130[a] above.

c. Claim 32[b]

140. Claim 32[b] recites “processing the security messages on the conditional access server; and....” Russ discloses this limitation, as I have discussed with respect to at least claim 130[b.i] above.

d. Claim 32[c]

141. Claim 32[c] recites “transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.” Russ discloses this limitation, as I have discussed with respect to at least claim 130[b.ii] above.

e. Claim 32[d.i]

142. Claim 32[d.i] recites “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 this limitation, as I have discussed with respect to at least claim 130[c.i] above.

f. Claim 32[d.ii]

143. Claim 32[d.ii] recites “the conditional access server authenticates clients

of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and....” Russ discloses this limitation, as I have discussed with respect to at least claim 130[c.ii] above.

g. Claim 32[d.iii]

144. Claim 32[d.iii] recites “wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.” Russ discloses this limitation, as I have discussed with respect to at least claim 130[c.iii] above.

h. Claim 33[pre]

145. Claim 33[pre] recites “The method of claim 32, wherein....” Russ discloses the method of claim 32, as I have discussed above.

i. Claim 33[a]

146. Claim 33[a] recites “the security messages comprise entitlement management messages.” Russ discloses this limitation, as I have discussed with respect to at least claim 131 above.

j. Claim 33[b]

147. Claim 33[b] recites “the conditional access server has a user key representing a subscriber of the primary security system; and....” Russ

discloses this limitation.

148. Russ discloses that DSCT 110 includes a private key used to decrypt messages, for example communications from headend 102, which uses DSCT 110's corresponding public key to encrypt communications.⁷⁶ DSCT 110 is a subscriber of headend 102 because, as discussed thoroughly above, DSCT 110 registers with, and becomes entitled to service instances through, headend 102.⁷⁷ DSCT 110's private key therefore represents a subscriber (*i.e.*, DSCT 110) of headend 102.

149. Thus, Russ discloses that the conditional access server has a user key representing a subscriber of the primary security system, as claimed.

k. Claim 33[c]

150. Claim 33[c] recites “said processing the entitlement management messages comprises: decrypting to obtain a service key of the primary security system.” Russ discloses this limitation.

151. Russ discloses that secure element 314 decrypts an EMM received from headend 102 to retrieve the MSK within. As I have discussed with respect to claim 130[c.iii], for example, the MSK is a key used by headend 102 to encrypt counter values to obtain the control word(s) that encrypt service instances—and used by

⁷⁶ Russ, 7:7-13.

⁷⁷ See, for example, Russ, 7:56-58.

DSCT 110 in the reverse to decrypt service instances.⁷⁸ Russ therefore discloses decrypting an EMM to obtain an MSK of headend 102.

152. Thus, Russ discloses that processing the entitlement management messages comprises: decrypting to obtain a service key of the primary security system, as claimed.

l. Claim 34

153. Claim 34 recites “The method of claim 32, wherein the access controlled data is protected using a digital rights management system.” Russ discloses this limitation, as I have discussed with respect to at least claim 131 above.

m. Claim 38[pre]

154. Claim 38[pre] recites “The method of claim 34, further comprising....” Russ discloses the method of claim 34, as I have discussed above.

n. Claim 38[a]

155. Claim 38[a] recites “receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and....” Russ discloses this limitation, as I have discussed with respect to at least claim 134[a] above.

o. Claim 38[b]

156. Claim 38[b] recites “descrambling the scrambled content according to

⁷⁸ Russ, 10:48-65, 11:37-46, 13:12-34, 22:40-45.

the entitlement control message.” Russ discloses this limitation, as I have discussed with respect to at least claim 134[b] above.

p. Claim 38[c]

157. Claim 38[b] recites “wherein the access controlled data comprises a result of descrambling the scrambled content.” Russ discloses this limitation, as I have discussed with respect to at least claim 134[c] above.

q. Claim 39[pre]

158. Claim 39[pre] recites “The method of claim 38, further comprising....” Russ discloses the method of claim 38, as I have discussed above.

r. Claim 39[a]

159. Claim 39[a] recites “storing, at the conditional access server, the content in an encrypted form.” Russ discloses this limitation, as I have discussed with respect to at least claim 135[a] above.

s. Claim 39[b]

160. Claim 39[b] recites “wherein the access controlled data is provided in response to a request from the secondary conditional access client.” Russ discloses this limitation, as I have discussed with respect to at least claim 135[b] above.

3. Invalidity of claims 66-68 and 72-73

161. Independent claim 66 is directed to “A non-transitory machine readable medium containing executable computer program instructions which when

executed by a data processing system cause said system to perform a method to process conditional access protection,” while independent 32 is directed to “A method to process conditional access protection” and independent claim 130 discussed above is directed to “A conditional access server.” Nevertheless, their limitations are substantially the same and therefore disclosed by the prior art for the same reasons. Below, I reference the relevant claim limitations of claims 32 or 130 and their dependent claims that disclose the same subject matter, and/or supplement with additional disclosures where limitations may differ.

a. Claim 66[pre]

162. Claim 66[pre] recites “A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, the method comprising....” Russ discloses this limitation.

163. Russ discloses that its system performs a method to process conditional access protection, as I have discussed with respect to at least claim 32 above.

164. Russ further discloses that the functions and methods discussed therein are “implemented in hardware, software, firmware, or a combination thereof,” for example with software stored in memory and executed by an instruction execution

system.⁷⁹ For example, the specific steps shown in Figures 5 and 6, reproduced below, are performed by processor 312, secure element 314, and/or cryptographic device 318.⁸⁰

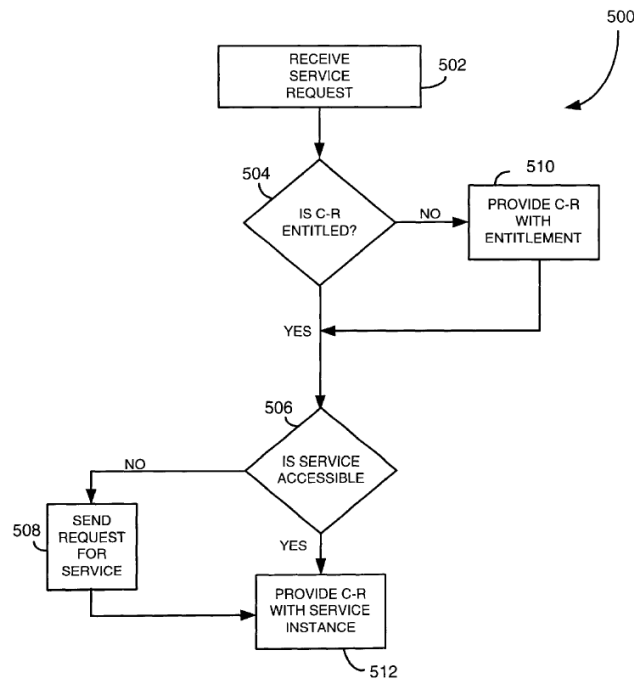


FIG. 5

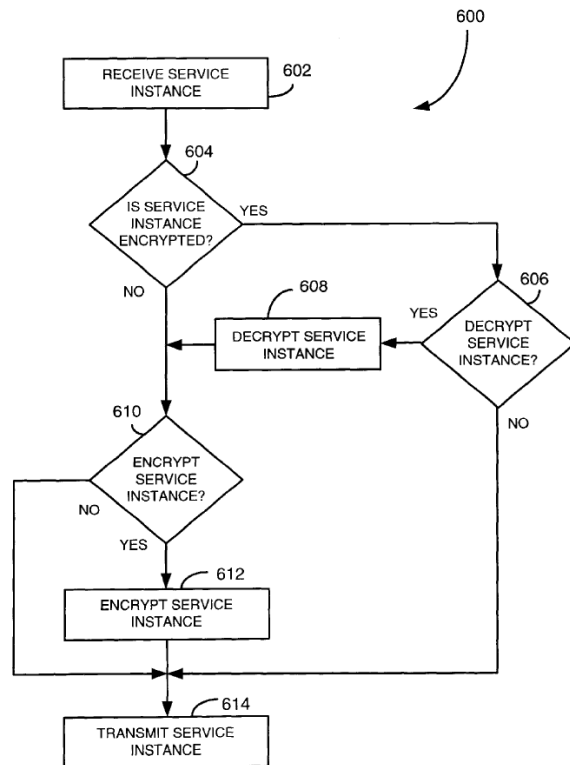


FIG. 6

165. Thus, Russ discloses non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, as claimed.

⁷⁹ Russ, 3:23-40; *see also* Russ, 16:13-26.

⁸⁰ Russ, 17:61-62, 19:43-45.

b. Claim 66[a]

166. Claim 66[a] recites “receiving, at a conditional access server, security messages of a primary security system in a first security domain.” Russ discloses this limitation, as I have discussed with respect to at least claims 130[pre] and 130[a] above.

c. Claim 66[b]

167. Claim 66[b] recites “processing the security messages on the conditional access server; and....” Russ discloses this limitation, as I have discussed with respect to at least claim 130[b.i] above.

d. Claim 66[c]

168. Claim 66[c] recites “transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.” Russ discloses this limitation, as I have discussed with respect to at least claim 130[b.ii] above.

e. Claim 66[d.i]

169. Claim 66[d.i] recites “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 this limitation, as I have discussed with respect to at least claim 130[c.i] above.

f. Claim 66[d.ii]

170. Claim 66[d.ii] recites “the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and....” Russ discloses this limitation, as I have discussed with respect to at least claim 130[c.ii] above.

g. Claim 66[d.iii]

171. Claim 66[d.iii] recites “wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.” Russ discloses this limitation, as I have discussed with respect to at least claim 130[c.iii] above.

h. Claim 67[pre]

172. Claim 67[pre] recites “The medium of claim 66, wherein....” Russ discloses the medium of claim 66, as I have discussed above.

i. Claim 67[a]

173. Claim 67[a] recites “the security messages comprise entitlement management messages.” Russ discloses this limitation, as I have discussed with

respect to at least claim 131 above.

j. Claim 67[b]

174. Claim 67[b] recites “the conditional access server has a user key representing a subscriber of the primary security system; and....” Russ discloses this limitation, as I have discussed with respect to at least claim 33[b] above.

k. Claim 67[c]

175. Claim 67[c] recites “said processing the entitlement management messages comprises: decrypting to obtain a service key of the primary security system.” Russ discloses this limitation, as I have discussed with respect to at least claim 33[c] above.

l. Claim 68

176. Claim 68 recites “The medium of claim 66, wherein the access controlled data is protected using a digital rights management system.” Russ discloses this limitation, as I have discussed with respect to at least claim 131 above.

m. Claim 72[pre]

177. Claim 72[pre] recites “The medium of claim 68, wherein the method further comprises....” Russ discloses the medium of claim 68, as I have discussed above.

n. Claim 72[a]

178. Claim 72[a] recites “receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and....” Russ discloses this limitation, as I have discussed with respect to at least claim 134[a] above.

o. Claim 72[b]

179. Claim 72[b] recites “descrambling the scrambled content according to the entitlement control message.” Russ discloses this limitation, as I have discussed with respect to at least claim 134[b] above.

p. Claim 72[c]

180. Claim 72[b] recites “wherein the access controlled data comprises a result of descrambling the scrambled content.” Russ discloses this limitation, as I have discussed with respect to at least claim 134[c] above.

q. Claim 73[pre]

181. Claim 73[pre] recites “The medium of claim 72, wherein the method further comprises....” Russ discloses the medium of claim 72, as I have discussed above.

r. Claim 73[a]

182. Claim 73[a] recites “storing, at the conditional access server, the content in an encrypted form.” Russ discloses this limitation, as I have discussed with

respect to at least claim 135[a] above.

s. Claim 73[b]

183. Claim 73[b] recites “wherein the access controlled data is provided in response to a request from the secondary conditional access client.” Russ discloses this limitation, as I have discussed with respect to at least claim 135[b] above.

B. Ground 2: Russ renders obvious claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135

184. As I discussed in Section II above, I have been informed that, when reviewing and analyzing the prior art in comparison to the '236 Patent's claims, the prior art may invalidate the '236 Patent's claims as being “anticipated” or as being “obvious” depending on the content and disclosure of the prior art references as understood by a person of ordinary skill in the art.

185. As I discussed in Section VIII.A, it is my opinion that Russ anticipates claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 of the '236 Patent. In other words, I understand Russ to disclose the conditional access server, the method to process conditional access protection, and the non-transitory machine readable medium as they are arranged in the claims of the '236 Patent. While Russ uses terms to describe some features as “examples,” or “alternative” embodiments, or “another” embodiment(s), I do not interpret these features to be individual, distinct, and independent features that must be viewed in a vacuum.

186. For instance, Russ states that “In an alternative embodiment, the headend 102 is in direct communication with hubs 104 and nodes 106 and in direct communication with subscriber locations 108.”⁸¹ Even though this is an “alternative” embodiment, a person of ordinary skill in the art would have recognized that this does not require the disclosure to be different from, opposite, incompatible, etc., with every other disclosure in Russ. Instead, a person of ordinary skill in the art would have recognized that this “alternative” is an example for implementing Russ’s system that includes headend 102 and subscriber locations 108 (which include DSCT 110 and client-receiver 122).⁸²

187. Nevertheless, to the extent that these disclosures may be found to be not “anticipating,” a person of ordinary skill in the art would have also determined that Russ renders obvious the ’236 Patent’s claims based on the same disclosures of the same headend, DSCT, client-receiver, and other related components discussed above. Russ teaches that its examples are merely “examples among other possible examples” or “example of implementations,” and “changes, modifications, or alterations to the invention as described may be made.”⁸³ Therefore, in implementing a system according to the disclosures in Russ, it would have been

⁸¹ Russ, 5:59-62.

⁸² Russ, 5:57-58.

⁸³ Russ, 2:52-54, 27:8-20.

obvious for a person of ordinary skill in the art to experiment with the various examples provided therein, which all relate to the interactions between the same headend, DSCT, and client-receivers, for example, to achieve a desired configuration.

188. Thus, Russ renders obvious, if not anticipates, claims 32-34, 38-39, 66-68, 72-73, 130-131, and 134-135 of the '236 Patent.

C. Ground 3: Russ in view of Robert renders obvious claims 35-36, 69-70, and 132-133

1. Motivation to combine the teachings of Russ and Robert

189. As I discussed in Section VIII.A above, Russ discloses that headend 102 provides service instances, entitlements, and other information to DSCT 110 (for example, EMMs, ECMs, MSKs); DSCT 110 manages its own local network that includes client-receiver 122; and, further, DSCT 110 and client-receiver 122 communicate with an encryption scheme that is specifically determined for use between them and that is determined when client-receiver 122 joins DSCT 110's network. Russ does not, however, dictate which encryption scheme must be used—such as SSL, DTCP, CPRM, TLS depending on the identity of the particular client-receiver⁸⁴—or every detail regarding every implementation, leaving the protocols

⁸⁴ For example, see Russ, 17:4-14.

to those “known to those skilled in the art.”⁸⁵ Therefore, a person of ordinary skill in the art implementing a system disclosed by Russ would have been motivated to look to known implementations for guidance, for example as taught by Robert.

190. Regarding dependent claim 132 of the '236 Patent: Claim 132 of the '236 Patent recites, for example, that “rights to the access controlled data are at least partially derived from the entitlement management messages.” Russ discloses that DSCT 110 derives rights to a service instance from a received EMM, for instance to entitle client-receiver 122 to the service instance.⁸⁶ However, to the extent that disclosure of rights is required with respect to the encryption scheme used between DSCT 110 and client-receiver 122, such as with DTCP, which is a digital rights management (DRM) scheme, Russ does not provide those details. Robert teaches the derivation of rights in the context of a system for accessing conditional access (CA) content on devices requiring DRM licenses and protection.⁸⁷ As I discuss in further detail below, Robert teaches to “interpret[] CA content protection information” and then “produc[e] a content license used for enforcing digital rights within [a] destination device” “based upon the interpreted [CA] content protection

⁸⁵ Russ, 17:12-14.

⁸⁶ Russ, 18:60-19:6.

⁸⁷ Robert, 8:56-11:59.

information.”⁸⁸ Robert explains that producing a DRM license in this way “maintain[s] security of the content and any associated protection content information (e.g., usage rights, access conditions, encryption keys, etc.).”⁸⁹ Therefore, a person of ordinary skill in the art, implementing Russ with DRM protection between DSCT 110 and client-receiver 122, which is otherwise not described in extensive detail by Russ, would have been motivated to implement details as taught by Robert, including providing DRM licenses with rights derived from entitlements received at DSCT 110 in order to ensure that protection information is maintained and not removed or evaded as it is transmitted from component to component throughout the system.

191. Regarding dependent claim 133 of the '236 Patent: Claim 133 of the '236 Patent recites, in part for example, that “the access controlled data comprises the control word.” Russ discloses an example in which client-receiver 122 decrypts service instances with control words.⁹⁰ Russ does not appear to detail, however, how client-receiver 122 generates control words—for example, if and when DSCT 110 transmits control words, control word indicators, ECMs, or other information that may be used by client-receiver 122 to generate control words. In addition to

⁸⁸ Robert, 12:8-26, Fig. 5.

⁸⁹ Robert, 4:50-65, 6:19-26.

⁹⁰ Russ, 26:16-28, 26:54-67.

Robert's teachings that I have discussed above—of interpreting rights for inclusion in DRM licenses—Robert teaches transmitting control words to a destination device while being protected in the DRM system.⁹¹ In this way, a destination device using DRM protocols is provided with information needed to decrypt CA-protected content.⁹² Therefore, a person of ordinary skill in the art would have been motivated to implement Russ in light of Robert's teachings and transmit control words from DSCT 110 to client-receiver 122, such that DSCT 110 is not required to decrypt or descramble the service instance for transmission to client-receiver 122. In this way, the process of decrypting or descrambling service instances is distributed to the client-receivers, and DSCT 110 saves time and resources for performing other functions or serving more devices.

192. A person of ordinary skill in the art would have had a reasonable expectation of success implementing Robert's teachings in Russ's system. As Russ and Robert both explain, various content protection protocols and encryption schemes were well-known in the art.⁹³ And, the combined teachings above generally use those known techniques, such as decrypting and encrypting or otherwise interpreting and generating CA or DRM content using known CA and DRM methods. Robert

⁹¹ Robert, 9:53-10:4.

⁹² Robert, 9:66-10:4.

⁹³ Russ, 17:7-14; Robert, 5:10-11.

further acknowledges that variations in timing or execution are obvious to persons of ordinary skill in the art.⁹⁴ Therefore, implementing Russ and Robert's teachings would have been well within the skill of a person of ordinary skill in the art.

2. Invalidity of claims 132-133

a. Claim 132

193. Claim 132 recites “The conditional access server of claim 131, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.” Russ in view of Robert renders obvious this limitation.

194. Russ discloses that rights to service instances are at least partially derived from EMMs. For example, Russ discloses that DSCT 110 receives an entitlement for a selected service instance in an EMM, processes the EMM, and then provides the entitlement to client-receiver 122.⁹⁵

195. And, as I have discussed in Section VIII.C.1 above, to the extent that disclosure of rights is required with respect to the encryption scheme used between DSCT 110 and client-receiver 122, such as with DTCP, it would have been obvious to a person of ordinary skill in the art to provide DRM licenses with rights

⁹⁴ Robert, 6:52-57.

⁹⁵ Russ, 18:52-65; see also Russ, 16:64-17:14, 17:61-18:66, 21:11-21, 24:1-24, 21:22-65.

derived from entitlements received at DSCT 110. In particular, Robert teaches to “interpret[] CA content protection information” and then “produc[e] a content license used for enforcing digital rights within [a] destination device” “based upon the interpreted [CA] content protection information.”⁹⁶

196. Thus, Russ in view of Robert renders obvious that rights to the access controlled data are at least partially derived from the entitlement management messages, as claimed.

b. Claim 133[pre]

197. Claim 133[pre] recites “The conditional access server of claim 131, wherein....” Russ discloses or renders obvious the conditional access server of claim 131, as I have discussed in Sections VIII.A and B.

c. Claim 133[a]

198. Claim 133[a] recites “the one or more communication interfaces are to receive an entitlement control message of the primary security system.” Russ discloses or renders obvious that the one or more communication interfaces are to receive an entitlement control message of the primary security system, as I have discussed with respect to at least claim 134[a] in Section VIII.A.1.

⁹⁶ Robert, 12:8-26, Fig. 5; *see also* Robert, 2:23-33, 4:18-26, 6:31-59, 8:56-11:59, Figs. 4A-4L.

d. Claim 133[b]

199. Claim 133[b] recites “the processor is to obtain a control word of the primary security system from the entitlement control message; and....” Russ discloses this limitation.

200. Russ discloses that when DSCT 110 is entitled to a service instance, its secure element 314 generates a control word from a control word indicator received via an ECM.⁹⁷ The ECM, for example, is generated by multi-transport stream transmitter receiver 228 of headend 102 and includes the counter value or control word indicator used to obtain the control word.⁹⁸ Russ therefore discloses that secure element 314 obtains a control word of headend 102 from the ECM.

201. Thus, Russ discloses that the processor is to obtain a control word of the primary security system from the entitlement control message, as claimed.

e. Claim 133[c]

202. Claim 133[c] recites “the access controlled data comprises the control word.” Russ in view of Robert renders obvious this limitation.

203. As I have discussed in Section VIII.C.1 above, it would have been obvious to a person of ordinary skill in the art to include control words in a DRM license transmitted from DSCT 110 to client-receiver 122, in Russ as taught by Robert,

⁹⁷ Russ, 23:39-67.

⁹⁸ Russ, 11:37-46, 13:12-34.

because doing so would provide client-receiver 122 the ability to decrypt or descramble service instances and further distribute processing loads across client-receivers.

204. Robert teaches, in particular, that in creating a DRM license, “receiver 410 could have included the appropriate keys (e.g., a list of CWs) in DRM license 430 when sent to destination device 420, such that destination device 420 can use the DRM license 430 to decrypt the CA-protected content 425 in its original form.”⁹⁹

205. Thus, Russ in view of Robert renders obvious that the access controlled data comprises the control word, as claimed.

3. Invalidity of claims 35-36 and 69-70

a. Claim 35

206. Claim 35 recites “The method of claim 34, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.” Russ in view of Robert renders obvious this limitation, as I have discussed with respect to at least claim 132 above.

b. Claim 36[pre]

207. Claim 36[pre] recites “The method of claim 34, further comprising....” Russ discloses or renders obvious the method of claim 34, as I have discussed in Sections VIII.A and B.

⁹⁹ Robert, 9:53-10:4, Fig. 4C; *see also* Robert, 6:31-59.

c. Claim 36[a]

208. Claim 36[a] recites “receiving, at the conditional access server, an entitlement control message of the primary security system; and....” Russ discloses or renders obvious receiving, at the conditional access server, an entitlement control message of the primary security system, as I have discussed with respect to at least claim 134[a] in Section VIII.A.1.

d. Claim 36[b]

209. Claim 36[b] recites “processing the entitlement control message on the conditional access server to obtain a control word of the primary security system.” Russ discloses this limitation as I have discussed with respect to at least claim 133[b] above.

e. Claim 36[c]

210. Claim 36[c] recites “wherein the access controlled data comprises the control word.” Russ in view of Robert renders obvious this limitation as I have discussed with respect to at least claim 133[c] above.

f. Claim 69

211. Claim 69 recites “The medium of claim 68, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.” Russ in view of Robert renders obvious this limitation, as I have discussed with respect to at least claim 132 above.

g. Claim 70[pre]

212. Claim 70[pre] recites “The medium of claim 68, wherein the method further comprises....” Russ discloses or renders obvious the medium of claim 68, as I have discussed in Sections VIII.A and B.

h. Claim 70[a]

213. Claim 70[a] recites “receiving, at the conditional access server, an entitlement control message of the primary security system; and....”

214. Russ discloses or renders obvious receiving, at the conditional access server, an entitlement control message of the primary security system, as I have discussed with respect to at least claim 134[a] in Section VIII.A.1.

i. Claim 70[b]

215. Claim 70[b] recites “processing the entitlement control message on the conditional access server to obtain a control word of the primary security system.” Russ discloses this limitation as I have discussed with respect to at least claim 133[b] above.

j. Claim 70[c]

216. Claim 70[c] recites “wherein the access controlled data comprises the control word.” Russ in view of Robert renders obvious this limitation as I have discussed with respect to at least claim 133[c] above.

D. Ground 4: Russ in view of Eskicioglu renders obvious claims 40-41, 43, 74-75, 77, and 136-137

1. Motivation to combine the teachings of Russ and Eskicioglu

217. As I discussed in Sections VIII.A and VIII.C.1 above, Russ discloses that headend 102 provides service instances, entitlements, and other information to DSCT 110 (for example, EMMs, ECMs, MSKs); DSCT 110 manages its own local network that includes client-receiver 122; and, further, DSCT 110 and client-receiver 122 communicate with an encryption scheme that is specifically determined for use between them and that is determined when client-receiver 122 joins DSCT 110's network. Russ does not, however, dictate which encryption scheme must be used—such as SSL, DTCP, CPRM, TLS depending on the identity of the particular client-receiver¹⁰⁰—or every detail regarding every implementation, leaving the protocols to those “known to those skilled in the art.”¹⁰¹ Moreover, as I discussed in Section VIII.C.1, Russ does not appear to provide specific details with respect to control words used by client-receiver 122, for example. Therefore, a person of ordinary skill in the art implementing a system disclosed by Russ would have been motivated to look to known implementations for guidance, for example as taught by Eskicioglu.

218. Claims 136 and 137 relate to generating a “substitutive entitlement control

¹⁰⁰ For example, see Russ, 17:4-14.

¹⁰¹ Russ, 17:12-14.

message as a replacement of the entitlement control message.” Eskicioglu teaches techniques related to one encryption scheme, “extended conditional access” (XCA) for protecting received CA content in local networks.¹⁰² In particular, Eskicioglu teaches rebundling received ECMs into LECMs, including control words, protected by a local key.¹⁰³ This LECM substitutes for the original received ECM and keeps content protected within the local network. Therefore, a person of ordinary skill in the art would have been motivated to configure the DSCT 110’s secure element, which processes security messages including ECMs,¹⁰⁴ to generate and transmit a substitutive ECM with a control word encrypted locally—*i.e.*, with DSCT 110’s key—as taught by Eskicioglu, to provide local protection for service instances and to ensure that services instances will not be later accessible outside the network. In implementing Eskicioglu’s teachings with Russ’s system (as I have discussed in Section VIII.A above), the service instance received from headend 102 would not need to be decrypted first by DSCT 110 because the LECM will include the same control words needed to decrypt or descramble the service instance.¹⁰⁵ Use of the LECM in this way would have therefore further saved time

¹⁰² Eskicioglu, 1:16-20, 2:1-40, 2:65-3:11, 3:50-4:15.

¹⁰³ Eskicioglu, 2:1-40, 7:41-53, 8:4-18.

¹⁰⁴ See my discussion of claims 130[b.i] and 133[b] in Sections VIII.A.1 and VIII.C.2 above.

¹⁰⁵ See Russ, 19:50-59.

and resources otherwise spent decrypting service instances at DSCT 110. And, as the LECM is a new substitutive ECM secured by DSCT 110's key, it furthers the goal of providing local protection by 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).

219. A person of ordinary skill in the art would have had a reasonable expectation of success implementing Eskicioglu's teachings in Russ's system. As described, Eskicioglu's "LECM" is similar to Russ's "ECM," the difference being that it is "local," and uses similar cryptographic functions. Additionally, the incorporation of ECM control words, discussed above, in DRM systems (as I have discussed, Russ discloses that DSCT 110 communicates with client-receiver 122 using DTCP protocols as an example) in various ways was a practice readily known to persons of ordinary skill in the art.¹⁰⁶ Indeed, including certain information, or decrypting/encrypting certain information, or not, makes use of existing data processing and cryptographic components existing in Russ. Therefore, implementing Russ and Eskicioglu's teachings would have been well within the skill of a person of ordinary skill in the art.

¹⁰⁶ Russ, 17:7-14; Robert, 6:31-59.

2. Invalidity of claims 136-137

a. Claim 136[pre]

220. Claim 136[pre] recites “The conditional access server of claim 130, wherein....” Russ discloses the conditional access server of claim 130, as I have discussed in Sections VIII.A and B.

b. Claim 136[a]

221. Claim 136[a] recites “the one or more communication interfaces are to receive entitlement control message of the primary security system.” Russ discloses or renders obvious that the one or more communication interfaces are to receive an entitlement control message of the primary security system, as I have discussed with respect to at least claim 134[a] in Section VIII.A.1.

c. Claim 136[b]

222. Claim 136[b] recites “the processor is to generate a substitutive entitlement control message as a replacement of the entitlement control message; and the access controlled data comprises the substitutive entitlement control message.” Russ in view of Eskicioglu renders obvious the limitation.

223. And, as I have discussed in Section VIII.D.1 above, it would have been obvious to a person of ordinary skill in the art to implement Russ’s system with DSCT 110’s secure element generating a substitutive ECM (or LECM) as a replacement of the ECM and to transmit the substitutive ECM (or LECM) as

access controlled data to client-receiver 122, as taught by Eskicioglu, to provide local protection of content.

224. In particular, Eskicioglu teaches that an access device receiving an ECM will rebundle the ECM into a local ECM (or LECM) by decrypting the ECM and re-encrypting the ECM using a local public key.¹⁰⁷ The LECM contains control words for decrypting content. For example, Eskicioglu teaches that a “CA module 42 recovers the control words (CW) or keys for the CA content and passes the CWs to converter module 46 which generates the necessary LECM.”¹⁰⁸

225. Thus, Russ in view of Eskicioglu renders obvious that the processor is to generate a substitutive entitlement control message as a replacement of the entitlement control message; and the access controlled data comprises the substitutive entitlement control message, as claimed.

d. Claim 137

226. Claim 137 recites “The conditional access server of claim 136, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.” Russ in view of Eskicioglu renders obvious the limitation.

227. As I have discussed with respect to at least claim 136[b] in the Section

¹⁰⁷ Eskicioglu, 7:41-46, 8:4-12, Claim 1, Fig. 4.

¹⁰⁸ Eskicioglu, 2:3-7, 8:19-30, Fig. 5.

above, Russ in view of Eskicioglu renders obvious that the substitutive ECM has a control word encrypted using a key of DSCT 110, which decrypts the ECM and re-encrypts information as an LECM.

228. Thus, Russ in view of Eskicioglu renders obvious that the substitutive entitlement control message has a control word encrypted using a key of the conditional access server, as claimed.

3. Invalidity of claims 40-41, 43, 74-75, and 77

a. Claim 40[pre]

229. Claim 40[pre] recites “The method of claim 32, further comprising....”

Russ discloses or renders obvious the method of claim 32, as I have discussed in Sections VIII.A and B.

b. Claim 40[a]

230. Claim 40[a] recites “receiving, at the conditional access server, an entitlement control message of the primary security system; and....” Russ discloses or renders obvious receiving, at the conditional access server, an entitlement control message of the primary security system, as I have discussed with respect to at least claim 134[a] in Section VIII.A.1.

c. Claim 40[b]

231. Claim 40[b] recites “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.” Russ in view of Eskicioglu renders obvious 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, as I have discussed with respect to at least claim 136[b] in Section VIII.D.2.

d. Claim 41

232. Claim 41 recites “The method of claim 40, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.” Russ in view of Eskicioglu renders obvious that the substitutive entitlement control message has a control word encrypted using a key of the conditional access server, as I have discussed with respect to at least claim 137 in Section VIII.D.2.

e. Claim 43

233. Claim 43 recites “The method of claim 41, wherein the entitlement control message and the substitutive entitlement control message have a same control word.” Russ in view of Eskicioglu renders obvious this limitation.

234. As I have discussed with respect to at least claim 136[b] in Section VIII.D.2,

Russ in view of Eskicioglu renders obvious the substitutive ECM (or LECM), wherein Eskicioglu teaches that “CA module 42 recovers the control words (CW) or keys for the CA content and passes the CWs to converter module 46 which generates the necessary LECM.”¹⁰⁹ Because the LECM is generated with the recovered control words, the ECM and LECM have the same control words.

235. Thus, Russ in view of Eskicioglu renders obvious that the entitlement control message and the substitutive entitlement control message have a same control word, as claimed.

f. Claim 74[pre]

236. Claim 74[pre] recites “The medium of claim 66, wherein the method further comprises....” Russ discloses or renders obvious the medium of claim 66, as I have discussed in Sections VIII.A and B.

g. Claim 74[a]

237. Claim 74[a] recites “receiving, at the conditional access server, an entitlement control message of the primary security system; and....” Russ discloses or renders obvious receiving, at the conditional access server, an entitlement control message of the primary security system, as I have discussed with respect to at least claim 134[a] in Section VIII.A.1.

¹⁰⁹ Eskicioglu, 2:3-7, 8:19-30, Fig. 5.

h. Claim 74[b]

238. Claim 74[b] recites “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.” Russ in view of Eskicioglu renders obvious 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, as I have discussed with respect to at least claim 136[b] in Section VIII.D.2.

i. Claim 75

239. Claim 75 recites “The medium of claim 74, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.” Russ in view of Eskicioglu renders obvious that the substitutive entitlement control message has a control word encrypted using a key of the conditional access server, as I have discussed with respect to at least claim 137 in Section VIII.D.2.

j. **Claim 77**

240. Claim 77 recites “The medium of claim 75, wherein the entitlement control message and the substitutive entitlement control message have a same control word.” Russ in view of Eskicioglu renders obvious that the entitlement control message and the substitutive entitlement control message have a same control word, as I have discussed with respect to at least claim 43 above.

IX. CONCLUSION

241. In summary, I conclude that Challenged Claims 32-36, 38-41, 43, 66-70, 72-75, 77, and 130-137 of the '236 Patent are anticipated and/or rendered obvious over the prior art references as discussed above.

242. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me.

243. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

244. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on June 14, 2024, in Johns Creek, Georgia.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "Anthony J. Wasilewski", written in black ink.

Anthony J. Wasilewski, Ph.D.