UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

ROKU, INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner.

_____

Case No. IPR2024-01024
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

IPR2025-00305
ASUS EX1003 Page 2

A. "access controlled data that is in an access controlled format and that is at least partially derived from the security messages" 22
B. Means-plus-function terms 25
1. "means for receiving" 25
VII. OVERVIEW OF THE PRIOR ART 26
A. Russ 26
B. Analogous Art 31
VIII. GROUNDS OF UNPATENTABILITY 31
A. Ground 1: Russ anticipates claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 32
1. Invalidity of claims 140-142 32
2. Invalidity of claims 48-50 and 57 54
3. Invalidity of claims 82-84 and 91 59
4. Invalidity of claims 116-118 and 125 63
B. Ground 2: Russ renders obvious claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 67
IX. CONCLUSION 70

IPR2025-00305
ASUS EX1003 Page 3

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")
1008	*VideoLabs, Inc. v. Roku, Inc.*, 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
1017	*VideoLabs, Inc. v. ASUSTeK Computer, Inc.*, Case No. 6:22-cv-00720 (W.D. Tex.), Dkt. No. 48, Plaintiff VideoLabs, Inc.'s Responsive Claim Construction Brief (Jun. 5, 2024)

I. INTRODUCTION

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 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 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 development 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.

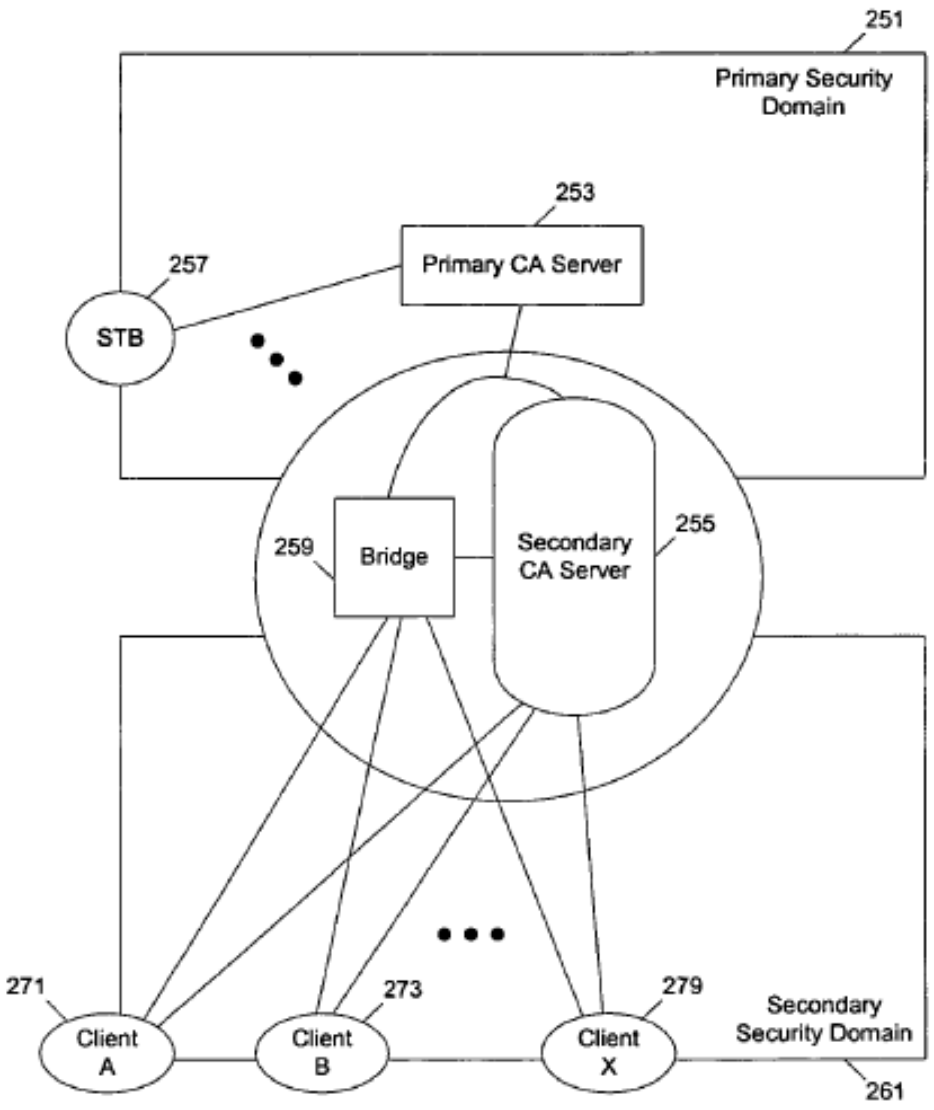

Fig. 2A

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, 474 (showing the language of claim 140 as of an amendment filed March 2, 2010), 509-513 (showing the Examiner's rejection of the pending claim).

[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 patently 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 48, 82, 116, and 140 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:[12]

[12] EX1008, 17-18.

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		

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.

B. Means-plus-function terms

52. I understand that certain claim terms of the ’236 Patent are expressed as “means for” performing certain functions.[13] 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.

1. “means for receiving”

53. “Means for receiving,” performing the function of receiving information, is recited in claim 116 as:

- Claim 116: “means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional

[13] I have also been informed that meaning of several of the ’236 Patent’s “means for” terms are in dispute and unresolved in district court litigation not involving Roku. EX1017.

access client being in a second security domain."

54. In the'236 Patent, a "communication interface" receives access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain.[14]

55. Accordingly, the structure in the specification linked to the claimed functions includes a communication interface and equivalents thereof.

VII. OVERVIEW OF THE PRIOR ART

56. 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

57. 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.

58. 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

[14] '236 Patent, claims 140, '236FH, 102.

after dynamic encryption scheme determination.[15] Service instances include, for example, audiovisual programs, Internet and telephone services, pay-per-view programming, and the like.[16] 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).

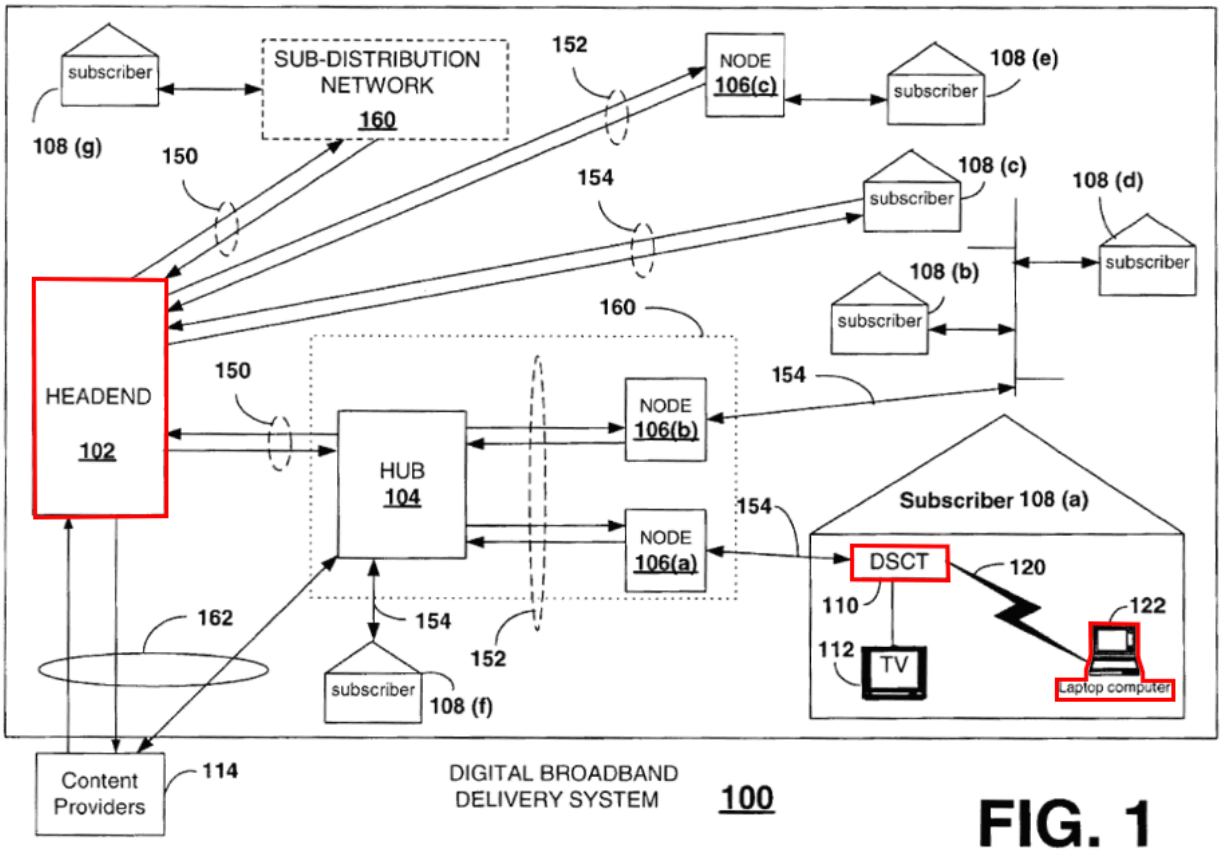

FIG. 1

59. Headend 102 includes conditional access authority (CAA) logic "for

[15] Russ, Abstract.

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

controlling access to the DBDS" by enabling DSCT 110 to receive entitlements for service instances.[17] In that regard, Russ discloses that DSCT 110 registers with the headend 102 and is entitled to service instances before receiving and accessing service instances.[18] 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.[19]

60. At subscriber location 108, DSCT 110 manages a local network, to which client-receiver 122 joins.[20] 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.[21] 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

---

[17] Russ, 8:8-11, 10:48-50.

[18] Russ, 7:56-58.

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

[20] Russ, 8:49-9:25, 16:32-42, 25:43-65.

[21] Russ, 16:64-17:34.

may be used.[22]

61. At the subscriber location 108, DSCT 110 provides service instances and related entitlements to client-receiver 122, and "DSCT 110 acts as an entitlement granting authority for the client-receiver 122" and grants/deletes client-receiver 122's entitlements to service instances based on information from headend 102.[23] Exemplary steps taken by DSCT 110 to service client-receiver 122 are shown in Figure 5 reproduced below.

[22] Russ, 17:7-14.

[23] Russ, 17:61-18:40, 18:60-65.

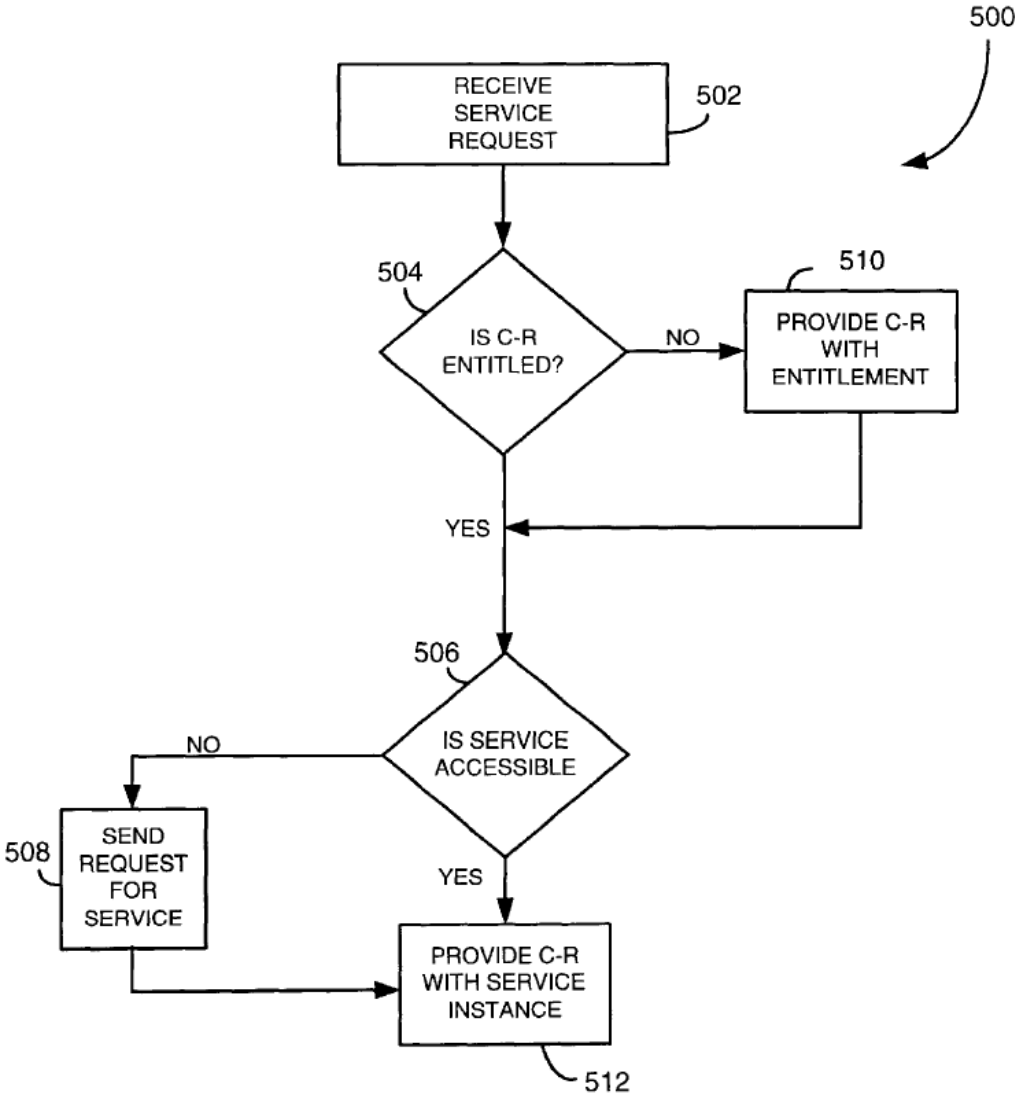

FIG. 5

Steps include, for example:[24]

- Receiving a request for a service instance (step 502);
- Determining if client-receiver 122 is entitled to the service instance

[24] Russ, 17:61-19:6.

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).

62. 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.[25]

B. Analogous Art

63. A person of ordinary skill in the art would have been aware of Russ and would have considered Russ to be in the same field as the '236 Patent. For example, the '236 Patent and Russ are both directed towards content distribution and management, including protection. *See* '236 Patent, 1:5-2:53; Russ, Abstract, 1:5-2:14.

VIII. GROUNDS OF UNPATENTABILITY

64. It is my opinion that the prior art references anticipate and/or render obvious

[25] Russ, 19:43-20:24, Fig. 6.

the Challenged Claims of the ’236 Patent as illustrated in the following Grounds:

- **Ground 1:** Russ anticipates claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142; and
- **Ground 2:** Russ renders obvious claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142.

65. 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 48-50, 57, 82-84, 91, 116-118, 125, and 140-142

1. Invalidity of claims 140-142

a. Claim 140[pre]

66. Claim 140[pre] recites “A secondary conditional access client.” Russ discloses this preamble, whether it limits the claim or not.

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

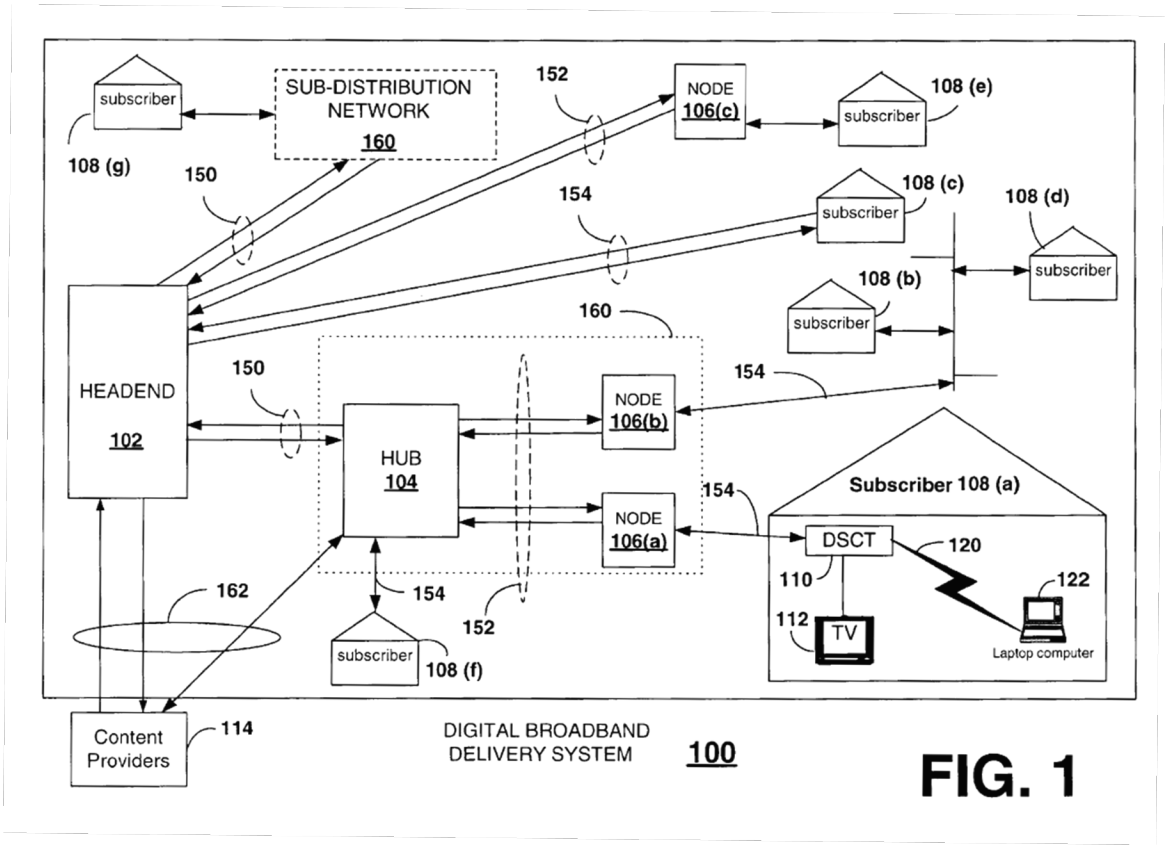

FIG. 1

68. 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.[26]

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

[26] 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.[27]

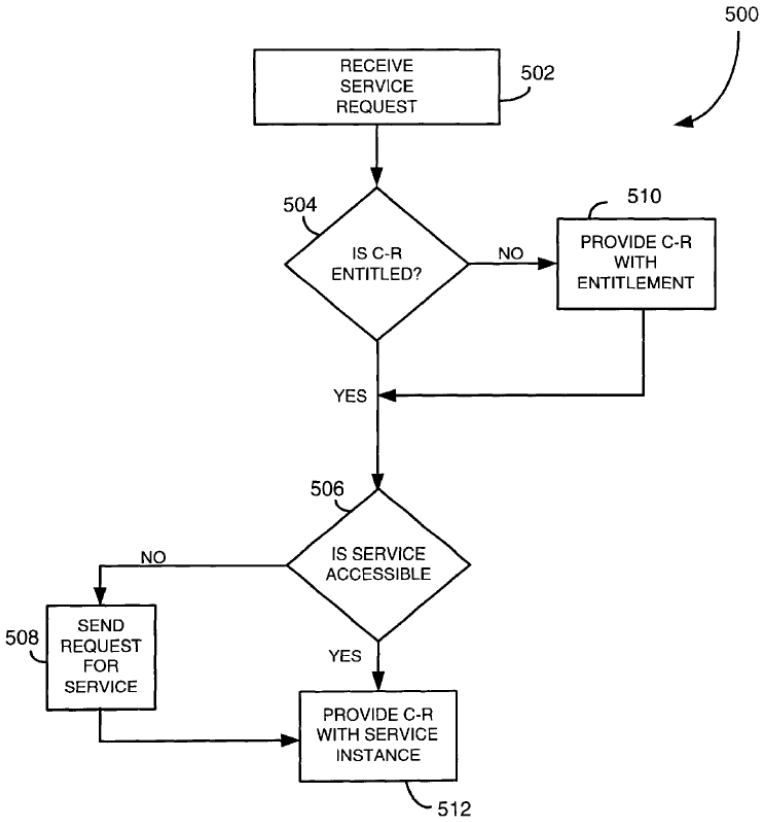

FIG. 5

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

[27] Russ, 17:61-18:66.

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

70. DSCT 110 is therefore a conditional access server, serving at least client-receiver 122, and client-receiver 122 is a conditional access client of DSCT 110. Client-receiver 122 is a "secondary" conditional access client because, for example, it operates with DSCT 110 in the second security domain, as I discuss further below with respect to at least claim elements 140[a.ii], 140[c.ii], and 140[c.iii].

71. Thus, Russ discloses a secondary conditional access client, as claimed.

b. Claim 140[a.i]

72. Claim 140[a.i] recites "a communication interface to receive, from a conditional access server through a network connection…." Russ discloses this limitation.

73. Russ shows an example of client-receiver 122 in Figure 9, reproduced below. As shown, client-receiver 122 includes transceiver 902 for communications with DSCT 110.

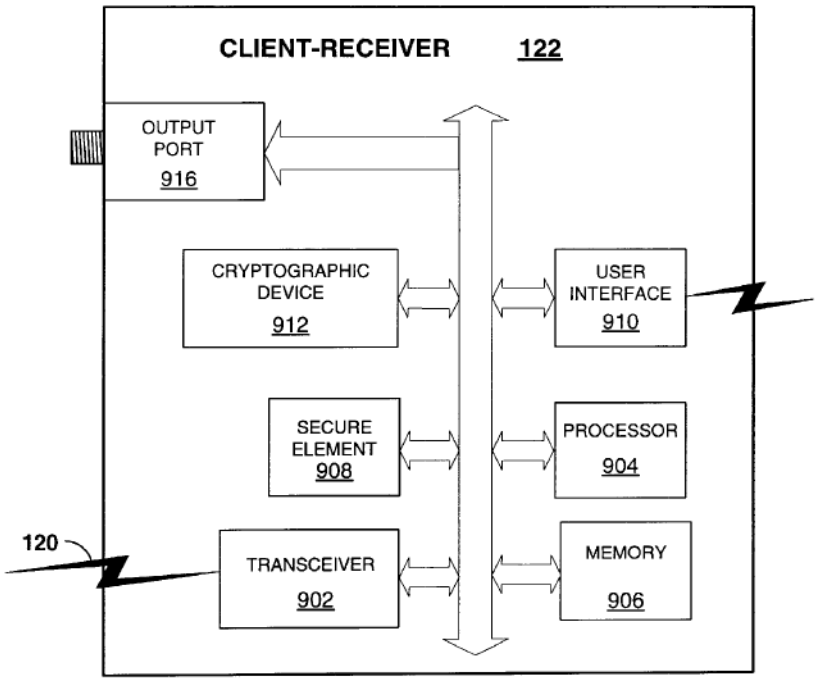

FIG. 9

74. For example, Russ states that "transceiver 902 receives information such as data, entitlements, authorizations, commands and service instances from the DSCT 110 via communication link 120."[28] The communication link 120 is, for example, a wired Ethernet link or a wireless IEEE 802.11 link, and communications are established when client-receiver 122 is brought into DSCT 110's local network.[29]

75. Thus, Russ discloses a communication interface to receive, from a

[28] Russ, 25:34-42.

[29] Russ, 8:38-48, 9:9-20.

conditional access server through a network connection, as claimed.

c. Claim 140[a.ii]

76. Claim 140[a.ii] recites that the communication interface is to receive "access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain." Russ discloses this limitation.

77. When client-receiver 122 joins DSCT 110's network, DSCT 110 dynamically determines an encryption scheme to protect data communicated with client-receiver 122.[30] Figure 4, reproduced below, shows steps that DSCT 110 performs to determine an encryption scheme to use with client-receiver 122.[31]

[30] Russ, 9:9-12, 16:64-17:14.

[31] Russ, 17:15-34.

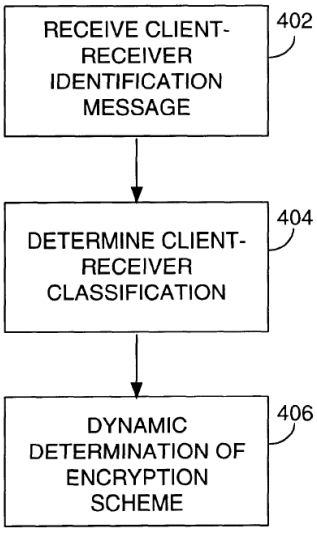

FIG. 4

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."[32] Indeed, a person of ordinary skill in the art would have been familiar with all those listed and more.

78. DSCT 110 will then use the determined encryption scheme—DTCP, for example—during communications with client-receiver 122 "to protect the privacy

[32] Russ, 17:7-14.

of the communication."[33] 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."[34] Content of EMMs communicated from DSCT 110 to client-receiver 122 are also encrypted.[35] 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.

79. 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.[36] And, for a particular requested service instance, an entitlement generator 236 in 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

---

[33] Russ, 16:64-17:14.

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

[35] Russ, 21:22-65, 24:1-24.

[36] Russ, 8:8-34, 15:46-52.

an EMM.[37] Russ therefore discloses that both service instances and EMMs are access controlled data at least partially derived from the security messages.

80. 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.[38]

81. Between DSCT 110 and headend 102, 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.[39] 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

---

[37] Russ, 18:52-65, 24:1-24.

[38] Russ, 20:25-53.

[39] Russ, 6:62-7:7, 7:56-58.

instances.[40] Headend 102 therefore represents a primary security system in a first security domain, different from the second security domain above, 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.

82. Thus, Russ discloses that that the communication interface is to receive access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain, as claimed.

83. 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." 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.[41] Therefore, Russ discloses partially deriving an access controlled format from an EMM.

84. Thus, Russ discloses, in an additional way, that that the communication interface is to receive access controlled data that is in an access controlled format

---

[40] Russ, 8:8-34, 10:48-65.

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

and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain, as claimed.

d. Claim 140[b]

85. Claim 140[b] recites "a processor coupled to the communication interface, the processor to process the access controlled data." Russ discloses this limitation.

86. Russ shows an example of client-receiver 122 in Figure 9, reproduced below. As shown, client-receiver 122 includes transceiver 902 for communications with DSCT 110.

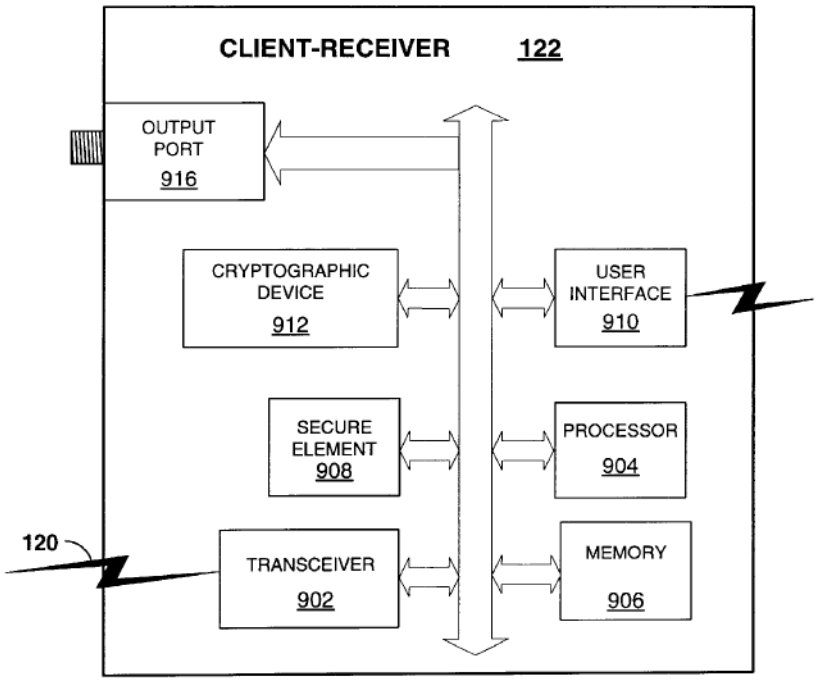

FIG. 9

87. Figure 9 also shows that transceiver 902 is coupled to processor 904, secure element 908, and cryptographic device 912.[42] Russ discloses that these components process access controlled data such as EMMs and service instances.

88. For example, Russ discloses that "secure element 908 … processes received EMMs."[43] Furthermore, secure element 908 "generates control words for the cryptographic device 912," which receives service instances from transceiver 902

[42] Russ, Fig. 9, 25:34-37.

[43] Russ, 26:16-28.

and decrypts them using the control words.[44] If a client-receiver 122 does not include a secure element 908, processor 904 performs its functions, including providing the control words for decrypting service instances.[45]

89. Thus, Russ discloses a processor coupled to the communication interface, the processor to process the access controlled data, as claimed.

e. Claim 140[c.i]

90. Claim 140[c.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.

91. 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.[46] When DSCT 110 registers with headend 102, which it must do before receiving 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

[44] Russ, 26:16-28, 26:61-64.

[45] Russ, 27:1-7.

[46] Russ, 7:21-39, 8:4-11.

database.[47] DSCT 110 is provided with a trusted public key for use.[48]

92. 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.[49] 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 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.

---

[47] Russ, 7:56-66.

[48] Russ, 7:58-66.

[49] Russ, 7:40-55.

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.

93. Thus, Russ discloses that 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, as claimed.

f. Claim 140[c.ii]

94. Claim 140[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.

95. Russ discloses that DSCT 110 authenticates client-receiver 122. As discussed with respect to at least claim 140[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.

96. 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:[50,51]

> 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.**

97. The DTCP certificate identifies a DTCP device and contains verifiable proof that the device is licensed to operate as a DTCP device.[52] Licensing in this case is

---

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

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

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

performed by a trusted licensing authority, such as the Digital Transmission Licensing Administrator ("DTLA"), which is the licensing organization of DTCP.[53]

98. 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 140[c.i] above.

99. 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.

g. Claim 140[c.iii]

100. Claim 140[c.iii] recites "wherein the conditional access server is configured to substitute the first security domain with the second security

[53] EX1011, [0107].

domain for the clients under the second root of trust." Russ discloses this limitation.

101. Russ discloses that service instances received at DSCT 110 are already encrypted by keys, for example by control words[54] that can be obtained by using a multi-session key (MSK) to encrypt a particular counter value.[55] 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.[56]

102. 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.

---

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

[55] Russ, 13:14-34.

[56] Russ, 11:37-46, 13:14-34.

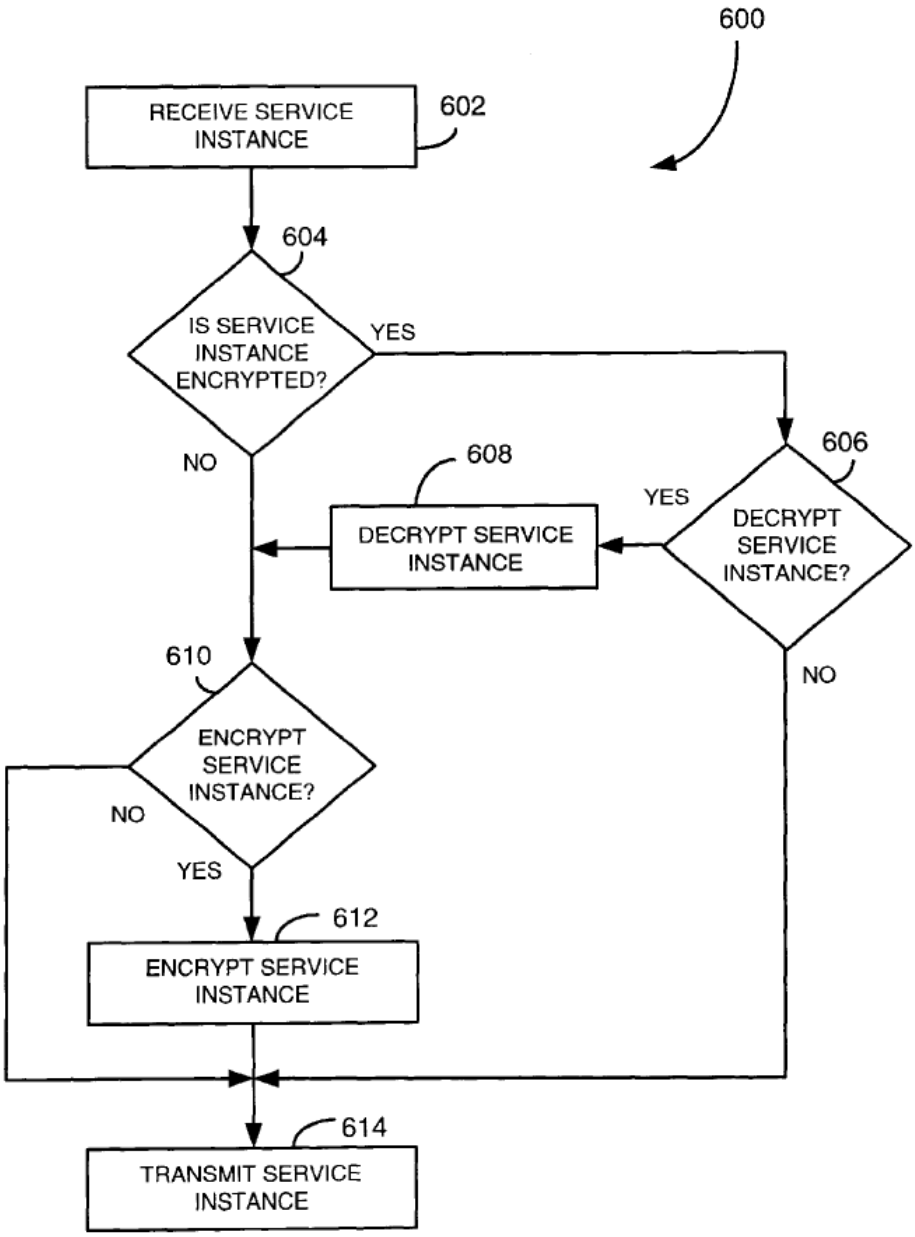

FIG. 6

Steps performed by DSCT 110 include,[57] for example:

[57] 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.

103. As I discussed above with respect to at least claim 140[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.

104. 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.

105. 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 141[pre]

106. Claim 141[pre] recites "The client of claim 140." Russ discloses the client

of claim 140, as I have discussed above.

i. Claim 141[a]

107. Claim 141[a] recites "wherein the security message is an entitlement management message." Russ discloses this limitation.

108. As I have discussed with respect to at least claims 140[a.ii] and 140[b] above, Russ discloses that DSCT 110 receives security messages such as entitlement management messages (EMMs).[58]

109. Thus, Russ discloses that the security message is an entitlement management message, as claimed.

j. Claim 141[b]

110. Claim 141[b] recites "wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system." Russ discloses this limitation.

111. Russ discloses that shared secrets between DSCT 110 and client-receiver 122 enable them to communication information securely. For example, Russ discloses "secrets that are shared between the DSCT 110 and the client-receiver 122" and "used for, among other things, encrypting service instances provided to the client-receiver 122, generating authentication tokens for messages transmitted to the client-receiver 122 and authenticating messages from the client-receiver

[58] *See* Russ, 8:4-37, 10:48-65, 25:17-25.

122."[59] Russ further discloses the secrets are "for authenticating messages and generating control words."[60] A person of ordinary skill in the art would have recognized that secrets used for such functions are keys, and because client-receiver 122 is an authenticated client of DSCT 110, as I have discussed with respect to at least claim 140 above, the keys are user keys representing a subscriber of DSCT 110.

112. Russ discloses the above because client-receiver 122 and DSCT 110 operate in the second security domain, as I have discussed with respect to at least claim 140 above. Client-receiver 122, which is in the second security domain, does not have the same relationship with headend 102, which is in the first security domain. Client-receiver 122 therefore does not have a user key representing a subscriber of the primary security system.

113. Thus, Russ discloses that the secondary conditional access client does not have a user key representing a subscriber of the primary security system, as claimed.

k. Claim 142

114. Claim 142 recites "The client of claim 140, wherein the access controlled format protects access to data using a digital rights management system."

---

[59] Russ, 20:47-53.

[60] Russ, 26:18-25.

Russ discloses this limitation.

115. I have discussed with respect to at least claims 140[a.ii] and 140[c.ii]-[c.iii] above, Russ discloses that between DSCT 110 and client-receiver 122, access controlled data is protected using DTCP protocols.[61] 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."[62]

116. Thus, Russ discloses that the access controlled format protects access to data using a digital rights management system, as claimed.

2. Invalidity of claims 48-50 and 57

117. Independent claim 48 is directed to "A method to process media content provided by a primary security system," while independent claim 140 discussed above is directed to "A secondary conditional access client." 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 140 and its dependent claims that disclose the same subject matter, and/or supplement with additional disclosures where limitations may differ.

---

[61] *See* Russ, 8:4-37, 10:48-65, 25:17-25.

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

a. Claim 48[pre]

118. Claim 48[pre] recites "A method to process media content provided by a primary security system, the method comprising…." Russ discloses this limitation.

119. As I have discussed with respect to claim 140 above, Russ discloses that client-receiver 122, along with DSCT 110 and headend 102, is included in a system DBDS 100 that processes service instances and provides them from the headend 102 to the DSCT 110 to the client-receiver 122.

120. Thus, Russ discloses a method to process media content provided by a primary security system.

b. Claim 48[a]

121. Claim 48[a] recites "receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain" Russ discloses this limitation, as I have discussed with respect to at least claims 140[a.i]-140[a.ii] above.

c. Claim 48[b.i]

122. Claim 48[b.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 140[c.i] above.

d. Claim 48[b.ii]

123. Claim 48[b.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 140[c.ii] above.

e. Claim 48[b.iii]

124. Claim 48[b.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 140[c.iii] above.

f. Claim 49[pre]

125. Claim 49[pre] recites "The method of claim 48." Russ discloses the method of claim 48, as I have discussed above.

g. Claim 49[a]

126. Claim 49[a] recites "wherein the security message is an entitlement message; and…." Russ discloses this limitation, as I have discussed with respect to at least claim 141[a] above.

h. Claim 49[b]

127. Claim 49[b] recites "wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system." Russ discloses this limitation, as I have discussed with respect to at least claim 141[b] above.

i. Claim 50

128. Claim 50 recites "The method of claim 48, wherein the access controlled format protects access to data using a digital rights management system." Russ discloses this limitation, as I have discussed with respect to at least claim 142 above.

j. Claim 57

129. Claim 57 recites "The method of claim 50, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system." Russ discloses this limitation.

130. As I discussed with respect to at least claims 140[a.ii] and 140[c.iii] 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.

131. Furthermore, Russ discloses that DSCT 110 must register with headend 102 and be entitled to service instances before receiving and accessing service instances.[63] And, those service instances are encrypted by headend 102 with control words, for example. In particular, Russ, describes that a "multi-transport stream transmitter/receiver 228 includes a counter that produces a numerical value every couple of seconds or so and an encryptor," and the "encryptor uses the MSK to encrypt the counter value to produce a control word" that is "used … as a key for encrypting a portion of the service instance."[64]

132. Thus, Russ discloses that the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system, as claimed.

---

[63] Russ, 7:56-58.

[64] Russ, 13:20-34; *see also* 12:47-13:19

3. Invalidity of claims 82-84 and 91

133. Independent claim 82 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 media content provided by a primary security system," while independent claim 48 is directed to "A method to process media content provided by a primary security system" and independent claim 140 discussed above is directed to "A secondary conditional access client." 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 48 or 140 and their dependent claims that disclose the same subject matter, and/or supplement with additional disclosures where limitations may differ.

a. Claim 82[pre]

134. Claim 82[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 media content provided by a primary security system, the method comprising…." Russ discloses this limitation.

135. Russ discloses that its system performs a method to process media content provided by a primary security system, as I have discussed with respect to at least

claim 48 above.

136. 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.[65]

137. 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 media content provided by a primary security system, as claimed.

b. Claim 82[a.i]

138. Claim 82[a.i] recites "receiving, at a secondary conditional access client from a conditional access server through a network connection." Russ discloses this limitation, as I have discussed with respect to at least claims 140[a.i] above.

c. Claim 82[a.ii]

139. Claim 82[a.ii] recites "access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain." Russ

[65] Russ, 3:23-40; *see also* Russ, 16:13-26.

discloses this limitation, as I have discussed with respect to at least claim 140[a.ii] above.

d. Claim 82[b.i]

140. Claim 82[b.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 140[c.i] above.

e. Claim 82[b.ii]

141. Claim 82[b.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 140[c.ii] above.

f. Claim 82[b.iii]

142. Claim 82[b.iii] recites "wherein the conditional access server is configured substitute the first security domain with the second security domain for the clients under the second root of trust." Russ discloses this limitation, as I have discussed with respect to at least claim 140[c.iii] above.

g. Claim 83[pre]

143. Claim 83[pre] recites "The medium of claim 82." Russ discloses the medium of claim 82, as I have discussed above.

h. Claim 83[a]

144. Claim 83[a] recites "wherein the security message is an entitlement management message; and…." Russ discloses this limitation, as I have discussed with respect to at least claim 141[a] above.

i. Claim 83[b]

145. Claim 83[b] recites "wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system." Russ discloses this limitation, as I have discussed with respect to at least claim 141[b] above.

j. Claim 84

146. Claim 84 recites "The medium of claim 82, wherein the access controlled format protects access to data using a digital rights management system." Russ discloses this limitation, as I have discussed with respect to at least claim 142 above.

k. Claim 91

147. Claim 91 recites "The medium of claim 84, wherein the access controlled data comprises a result of descrambling media content scrambled

by a conditional access system of the primary security system." Russ discloses this limitation, as I have discussed with respect to at least claim 57 above.

4. Invalidity of claims 116-118 and 125

148. Independent claim 116 is directed to "A data processing system to process media content provided by a primary security system," while independent claim 82 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 media content provided by a primary security system," independent claim 48 is directed to "A method to process media content provided by a primary security system" and independent claim 140 discussed above is directed to "A secondary conditional access client." 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 48, 82, or 140 and their dependent claims that disclose the same subject matter, and/or supplement with additional disclosures where limitations may differ.

a. Claim 116[pre]

149. Claim 116[pre] recites "A data processing system to process media content provided by a primary security system, the method comprising…." Russ discloses this limitation.

150. As I have discussed for at least claims 140[pre], 48[pre], and 82[pre], Russ

discloses a DBDS 100 including DSCT 110 and client-receiver 122 that performs a method to process media content provided by a primary security system including headend 102.

151. Thus, Russ discloses a data processing system to process media content provided by a primary security system, as claimed.

b. Claim 116[a]

152. Claim 116[a] recites "means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain." Russ discloses this limitation, as I have discussed with respect to at least claims 140[a.i]-[a.ii] above.

153. Furthermore, transceiver 902 is a form of communication interface and therefore satisfies this limitation's "means for receiving." As I discussed in Section VI.B.1 above, the "means for receiving" includes a communication interface and equivalents thereof.

154. Thus, Russ discloses means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially

derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain.

c. Claim 116[b.i]

155. Claim 116[b.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, as I have discussed with respect to at least claim 140[c.i] above.

d. Claim 116[b.ii]

156. Claim 116[b.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 140[c.ii] above.

e. Claim 116[b.iii]

157. Claim 116[b.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 140[c.iii] above.

f. Claim 117[pre]

158. Claim 117[pre] recites "The data processing system of claim 116." Russ discloses the data processing system of claim 116, as I have discussed above.

g. Claim 117[a]

159. Claim 117[a] recites "wherein the security message is an entitlement management message; and…." Russ discloses this limitation, as I have discussed with respect to at least claim 141[a] above.

h. Claim 117[b]

160. Claim 117[b] recites "wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system." Russ discloses this limitation, as I have discussed with respect to at least claim 141[b] above.

i. Claim 118

161. Claim 118 recites "The data processing system of claim 116, wherein the access controlled format protects access to data using a digital rights management system." Russ discloses this limitation, as I have discussed with respect to at least claim 142 above.

j. Claim 125

162. Claim 125 recites "The data processing system of claim 118, wherein the access controlled data comprises a result of descrambling media content

scrambled by a conditional access system of the primary security system." Russ discloses this limitation, as I have discussed with respect to at least claim 57 above.

B. Ground 2: Russ renders obvious claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142

163. 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.

164. As I discussed in Section VIII.A, it is my opinion that Russ anticipates claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 of the '236 Patent. In other words, I understand Russ to disclose the secondary conditional access client, the method to process media content, the non-transitory machine readable medium, and the data processing system 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.

165. 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."[66] 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).[67]

166. 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."[68] Therefore, in implementing a system according to the disclosures in Russ, it would have been 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

---

[66] Russ, 5:59-62.

[67] Russ, 5:57-58.

[68] Russ, 2:52-54, 27:8-20.

headend, DSCT, and client-receivers, for example, to achieve a desired configuration.

167. Thus, Russ renders obvious, if not anticipates, claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 of the ’236 Patent.

IX. CONCLUSION

168. In summary, I conclude that Challenged Claims 48-50, 57, 82-84, 91, 116-118, 125, and 140-142 of the ’236 Patent are anticipated and/or rendered obvious over the prior art references as discussed above.

169. 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.

170. 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.

171. 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,

Anthony J. Wasilewski, Ph.D.